A 12-2702

CLERK, U.S. DISTRICT COURT
RECEIVED
OCT 5 2012
EASTERN DIST. OF TEXAS

AO 440 (Rev. 12/09) Summons in a Civil Action

AD 611 Bakgr. Dar 013573/12
2012 -09- 26
POLISMYNDIGHETEN I STOCKHOLMS LÄN
Delgivningssektionen

UNITED STATES DISTRICT COURT

for the

Eastern District of Texas

Uniloc USA, Inc. and Uniloc Luxembourg S.A.

Plaintiff

v.

Mojang AB

Defendant

Civil Action No. 6:12-cv-470

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Mojang AB

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Barry J. Bumgardner
NELSON BUMGARDNER CASTO, P.C.,
3131 West 7th Street, Suite 300
Fort Worth, Texas 76107
Phone: (817) 377-9111

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: 7/23/12

UNITED STATES DISTRICT COURT * EASTERN DISTRICT OF TEXAS *

Signature of Clerk or Deputy Clerk

Intygas:
27/9-12
Datum
SALAH BOUDIAF
Stämningsman
Polismyndigheten i Stockholms län
Utlämnarens namnteckning
Namnförtydligande, titel

Att ovanstående handling
har delgivits härmed

Jacob Parser
Styrelseledamot

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

UNILOC USA, INC. and UNILOC LUXEMBOURG S.A.,	§	
Plaintiffs,	§	CIVIL ACTION NO. 6:12-cv-470
	§	**JURY TRIAL DEMANDED**
v.	§	
MOJANG AB,	§	
Defendant.	§	

PLAINTIFFS' ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs Uniloc USA, Inc. ("Uniloc USA") and Uniloc Luxembourg S.A. ("Uniloc Luxembourg") (collectively, "Uniloc") file this Original Complaint against Mojang AB for infringement of U.S. Patent No. 6,857,067 ("the '067 patent").

THE PARTIES

1. Uniloc USA, Inc. ("Uniloc USA") is a Texas corporation with its headquarters and principal place of business at Legacy Town Center I, Suite 380, 7160 Dallas Parkway, Plano, Texas 75024. Uniloc USA also maintains a place of business at 315 North Broadway, Suite 307, Tyler, Texas 75702.

2. Uniloc Luxembourg S.A. ("Uniloc Luxembourg") is a corporation organized and existing under the laws of Luxembourg with its principal place of business at 15, rue Edward Steichen, L-2540, Luxembourg.

3. Uniloc Luxembourg and Uniloc USA are collectively referred to as "Uniloc." Uniloc researches, develops, manufactures and licenses information security technology

solutions, platforms and frameworks, including solutions for securing software applications and digital content. Uniloc's patented technologies enable software and content publishers to securely distribute and sell their high-value technology assets with minimum burden to their legitimate end users. Uniloc's technology is used in several markets, including software and game security, identity management, intellectual property rights management, and critical infrastructure security.

4. Mojang AB ("Mojang") is organized and exists under the laws of Sweden with its principal place of business in Stockholm, Sweden. Upon information and belief, Mojang does business in the State of Texas and in the Eastern District of Texas.

JURISDICTION AND VENUE

5. Uniloc brings this action for patent infringement under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1338(a), and 1367.

6. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). On information and belief, Defendant is deemed to reside in this judicial district, has committed acts of infringement in this judicial district, has purposely transacted business involving its accused products in this judicial district and/or, has regular and established places of business in this judicial district.

7. Defendant is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and judicial district, including: (A) at least part of its infringing activities alleged herein; and (B) regularly doing or soliciting business, engaging in other persistent conduct, and/or deriving substantial revenue from goods sold and services provided to Texas residents.

COUNT I
(INFRINGEMENT OF U.S. PATENT NO. 6,857,067)

8. Uniloc incorporates paragraphs 1 through 7 herein by reference.

9. Uniloc Luxembourg is the owner, by assignment, of the '067 patent, entitled "SYSTEM AND METHOD FOR PREVENTING UNAUTHORIZED ACCESS TO ELECTRONIC DATA." A true and correct copy of the '067 patent is attached as Exhibit A.

10. Uniloc USA is the exclusive licensee of the '067 patent with ownership of all substantial rights in the '067 patent, including the right to grant sublicenses, exclude others and to enforce, sue and recover damages for past and future infringements.

11. The '067 patent is valid, enforceable and was duly issued in full compliance with Title 35 of the United States Code.

12. Mojang is directly infringing one or more claims of the '067 patent in this judicial district and elsewhere in Texas, including at least claim 107, without the consent or authorization of Uniloc, by or through making, using, offering for sale, selling and/or importing Android based applications for use on cellular phones and/or tablet devices that require communication with a server to perform a license check to prevent the unauthorized use of said application, including, but not limited to, Mindcraft.

13. Uniloc has been damaged as a result of Defendant's infringing conduct described in this Count. Defendant is, thus, liable to Uniloc in an amount that adequately compensates it for Defendant's infringements, which, by law. cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Uniloc hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

Uniloc requests that the Court find in its favor and against Defendant, and that the Court grant Uniloc the following relief:

a. Judgment that one or more claims of the '067 patent has been infringed, either literally and/or under the doctrine of equivalents, by Defendant;

b. Judgment that Defendant account for and pay to Uniloc all damages to and costs incurred by Uniloc because of Defendant's infringing activities and other conduct complained of herein;

c. Judgment that Defendant account for and pay to Uniloc a reasonable, on-going, post judgment royalty because of Defendant's infringing activities and other conduct complained of herein;

d. That Uniloc be granted pre-judgment and post-judgment interest on the damages caused by Defendant's infringing activities and other conduct complained of herein; and

e. That Uniloc be granted such other and further relief as the Court may deem just and proper under the circumstances.

Dated: July 20, 2012

Respectfully submitted,

/s/ Barry J. Bumgardner (w/permission Wesley Hill)
Barry J. Bumgardner
Lead Attorney
Texas State Bar No. 00793424
Steven W. Hartsell
Texas State Bar No. 24040199
NELSON BUMGARDNER CASTO, P.C.
3131 West 7th Street, Suite 300
Fort Worth, Texas 76107
Phone: (817) 377-9111
Fax: (817) 377-3485

James L. Etheridge
Texas Bar No. 24059147
ETHERIDGE LAW GROUP, PLLC
2600 E. Southlake Blvd., Suite 120 / 324
Southlake, Texas 76092
Telephone: (817) 470-7249
Facsimile: (817) 887-5950
Jim@EtheridgeLaw.com

T. John Ward, Jr.
Texas State Bar No. 00794818
E-mail: jw@wsfirm.com
J. Wesley Hill
Texas State Bar No. 24032294
E-MAIL: WH@WSFIRM.COM
WARD & SMITH LAW FIRM
P.O. Box 1231
1127 Judson Rd., Ste. 220
Longview, Texas 75606-1231
(903) 757-6400
(903) 757-2323 (fax)

Attorneys for Plaintiffs
Uniloc USA, Inc. and Uniloc Luxembourg S.A.

JS 44 (Rev. 09/11)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
UNILOC USA, INC. and UNILOC LUXEMBOURG S.A.

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Barry J. Bumgardner, NELSON BUMGARDNER CASTO, P.C., 3131 West 7th Street, Suite 300, Fort Worth, Texas 76107, Phone: (817) 377-9111

DEFENDANTS
MOJANG AB

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff) and One Box for Defendant) (For Diversity Cases Only)*

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Med. Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS
- ☐ 510 Motions to Vacate Sentence Habeas Corpus:
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Mgmt. Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Empl. Ret. Inc. Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus - Alien Detainee (Prisoner Petition)
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☒ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*
☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district *(specify)* ☐ 6 Multidistrict Litigation

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
35 U.S.C. §§ 271, 281, and 284-285
Brief description of cause:
patent infringement

VII. REQUESTED IN COMPLAINT: ☐ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23 DEMAND $ CHECK YES only if demanded in complaint: JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions)*: JUDGE PLEASE SEE ATTACHED DOCKET NUMBER PLEASE SEE ATTACHED

DATE 07/20/2012

SIGNATURE OF ATTORNEY OF RECORD /s/ Barry J. Bumgardner (w/permission Wesley Hill)

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

RELATED CASES

DOCKET NUMBERS:

6:12-cv-462 - JUDGE NOT ASSIGNED
6:12-cv-463 – JUDGE NOT ASSIGNED
6:12-cv-464 – JUDGE NOT ASSIGNED
6:12-cv-466 – JUDGE NOT ASSIGNED
6:12-cv-467 – JUDGE NOT ASSIGNED
6:12-cv-468 – JUDGE NOT ASSIGNED
6:12-cv-469 – JUDGE NOT ASSIGNED

Exhibit "A"

US006857067B2

(12) **United States Patent**
Edelman

(10) **Patent No.: US 6,857,067 B2**
(45) **Date of Patent: Feb. 15, 2005**

(54) **SYSTEM AND METHOD FOR PREVENTING UNAUTHORIZED ACCESS TO ELECTRONIC DATA**

(76) Inventor: **Martin S. Edelman**, 11 Lake Ontario La., Morganville, NJ (US) 07751

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 641 days.

(21) Appl. No.: **09/792,045**

(22) Filed: **Feb. 26, 2001**

(65) **Prior Publication Data**

US 2002/0029347 A1 Mar. 7, 2002

Related U.S. Application Data

(60) Provisional application No. 60/229,934, filed on Sep. 1, 2000.

(51) **Int. Cl.**[7] **G06F 1/26**

(52) **U.S. Cl.** **713/1.55**; 713/182; 713/200; 713/201

(58) **Field of Search** 713/155, 182, 713/200, 201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,502,764	A	3/1996	Naccache	380/23
5,826,013	A	10/1998	Chou et al.	395/186
5,844,497	A	12/1998	Gray	340/825.34
5,933,498	A	8/1999	Schneck et al.	380/4
5,935,246	A	8/1999	Benson	713/200
5,940,504	A	8/1999	Griswold	380/4
5,956,404	A	9/1999	Schneier et al.	380/25
5,987,134	A	11/1999	Shin et al.	380/25
6,008,737	A	12/1999	Deluca et al.	340/825.34
6,009,401	A	12/1999	Horstmann	705/1
6,009,525	A	12/1999	Horstmann	713/200
6,021,438	A	2/2000	Duvvoori et al.	709/224
6,023,766	A	2/2000	Yamamura	713/201
6,029,145	A	2/2000	Barritz et al.	705/34
6,035,402	A	3/2000	Vaeth et al.	713/201
6,047,242	A	4/2000	Benson	702/35
6,049,789	A	4/2000	Frison et al.	705/59
6,067,582	A	5/2000	Smith et al.	710/5
6,073,123	A	6/2000	Staley	705/58
6,078,909	A	6/2000	Knutson	705/59
6,087,955	A	7/2000	Gray	340/825.34
6,101,606	A	8/2000	Diersch et al.	713/201
6,128,741	A	10/2000	Goetz et al.	713/200

OTHER PUBLICATIONS

Charles Cagliostro, "Rosy Outlook Predicted for US Smart Card Market", Card Forum International, pp. 45–47, Nov./Dec. 1999.

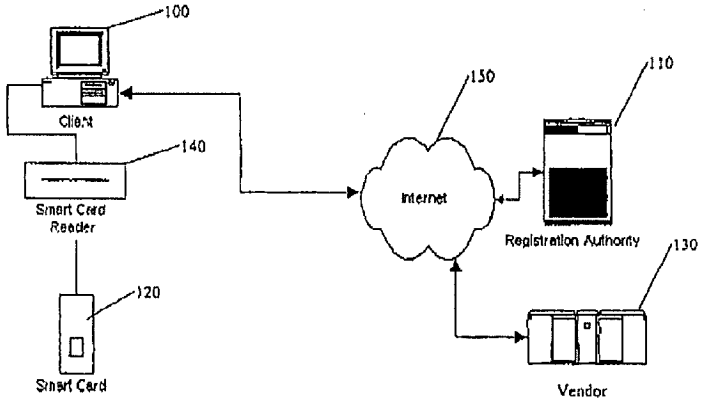
Carol H. Pancher, "Smart Cards", Scientific American, pp. 1–10, Aug. 1996.

Primary Examiner—Thomas R. Peeso
(74) *Attorney, Agent, or Firm*—Fitzpatrick, Cella, Harper & Scinto

(57) **ABSTRACT**

A system and method are provided for preventing unauthorized access to electronic data stored on an electronic device. A portable licensing medium is configured to communicate with the electronic device for storing license data. The license data is used to determine whether to allow access to the electronic data. A registration authority communicates with the electronic device. The registration authority has a database of verification data for verifying the license data stored on the licensing medium and provides updated license data to the licensing medium.

113 Claims, 9 Drawing Sheets



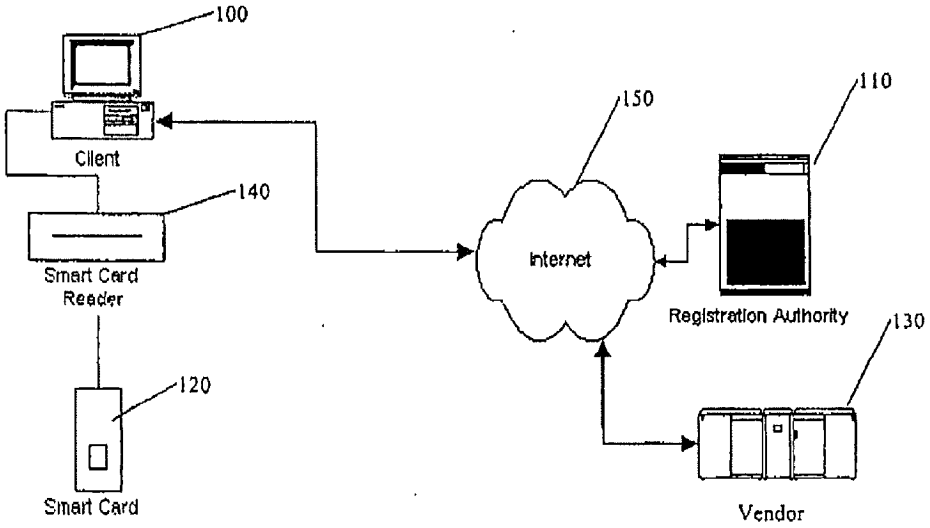

100
Client
140
Smart Card
Reader
120
Smart Card
150
Internet
110
Registration Authority
130
Vendor

Fig. 1

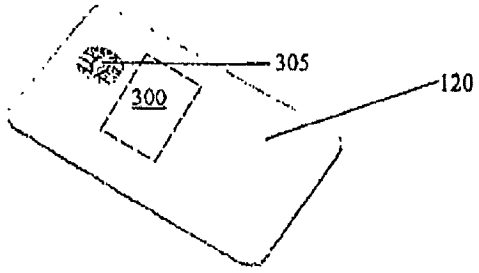

305
300
120

Fig. 2

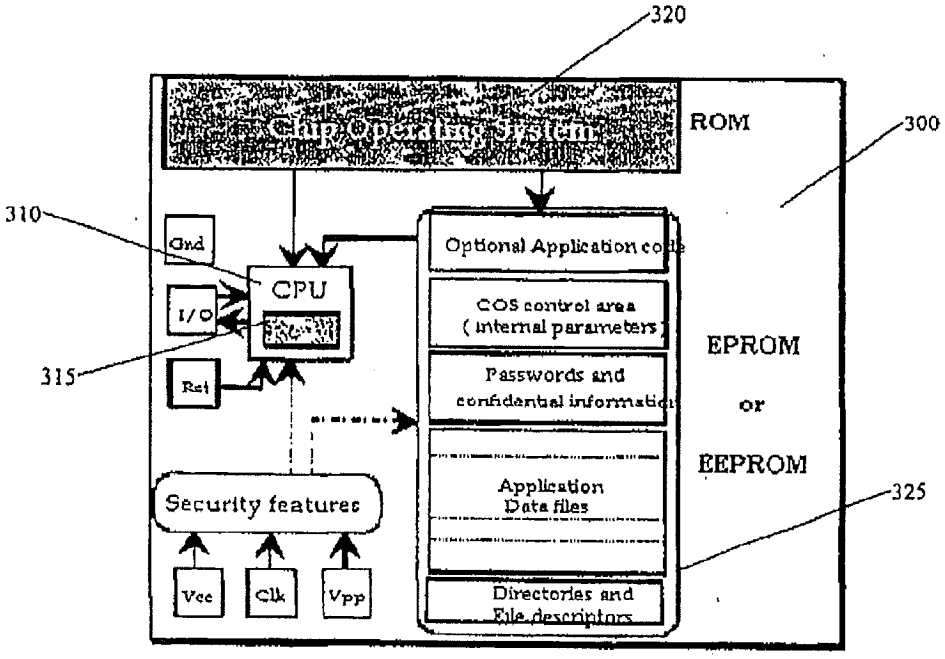

320
Chip Operating System
ROM
300
310
Gnd
CPU
I/O
Rst
315
Optional Application code
COS control area (internal parameters)
Passwords and confidential information
EPROM
or
EEPROM
Application Data files
325
Security features
Vcc
Clk
Vpp
Directories and File descriptors

Fig. 3

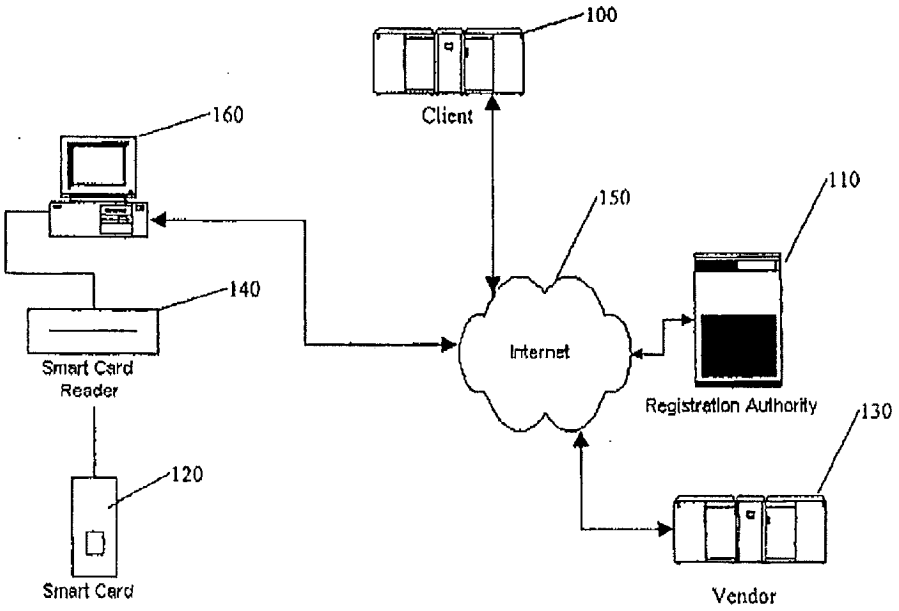

100
Client
160
150
110
140
Internet
Smart Card
Reader
Registration Authority
130
120
Smart Card
Vendor

Fig. 4

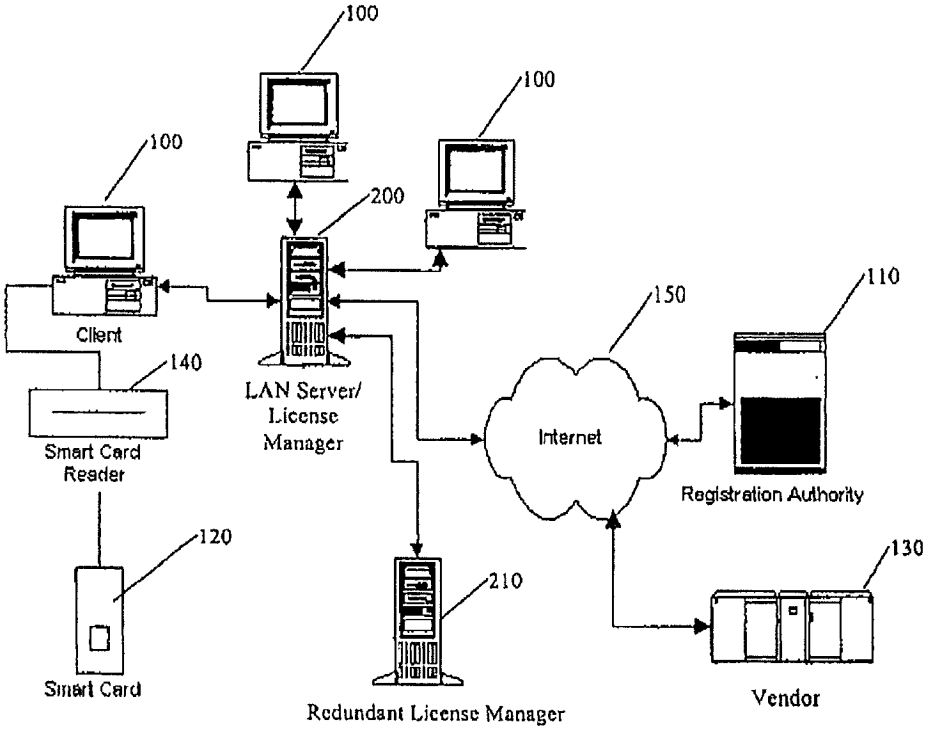

100
100
100
200
Client
140
Smart Card Reader
LAN Server/ License Manager
150
Internet
110
Registration Authority
120
Smart Card
210
Redundant License Manager
130
Vendor

Fig. 5

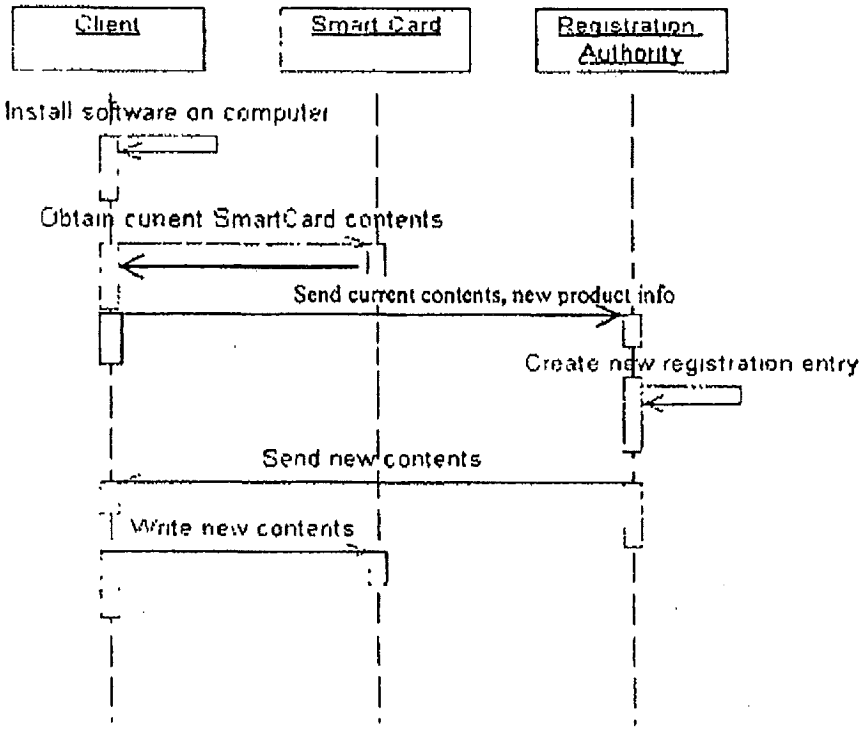

Client
Smart Card
Registration Authority
Install software on computer
Obtain cunent SmartCard contents
Send current contents, new product info
Create new registration entry
Send new contents
Write new contents

Fig. 6

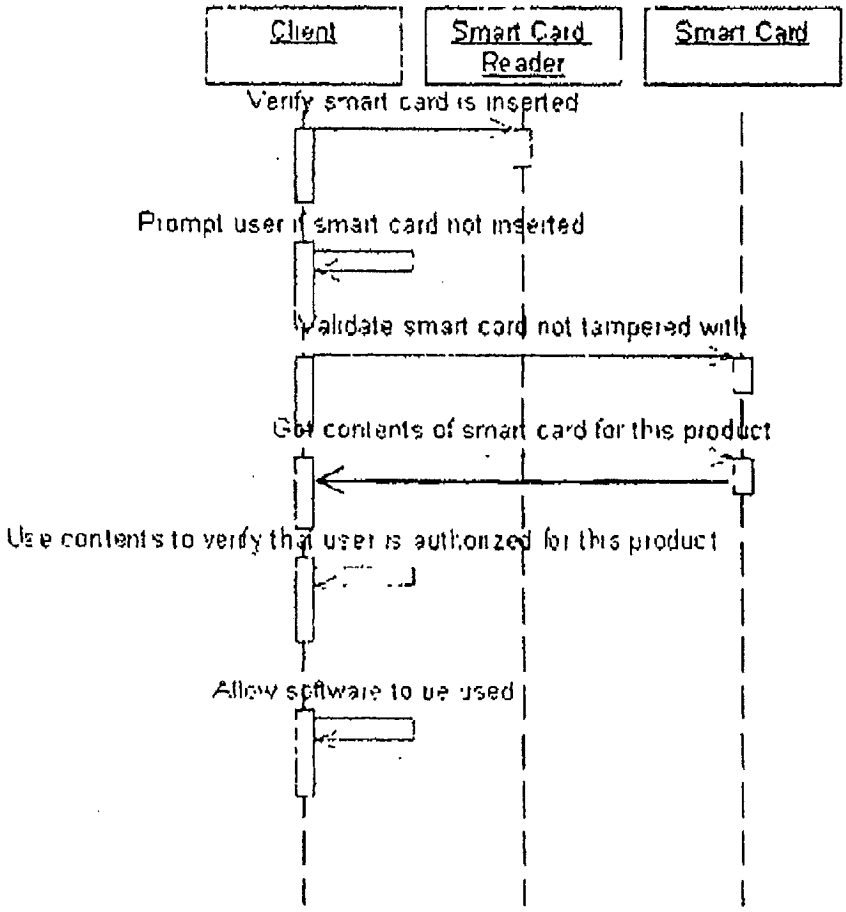

Client
Smart Card Reader
Smart Card
Verify smart card is inserted
Prompt user if smart card not inserted
Validate smart card not tampered with
Get contents of smart card for this product
Use contents to verify that user is authorized for this product
Allow software to be used

Fig. 7

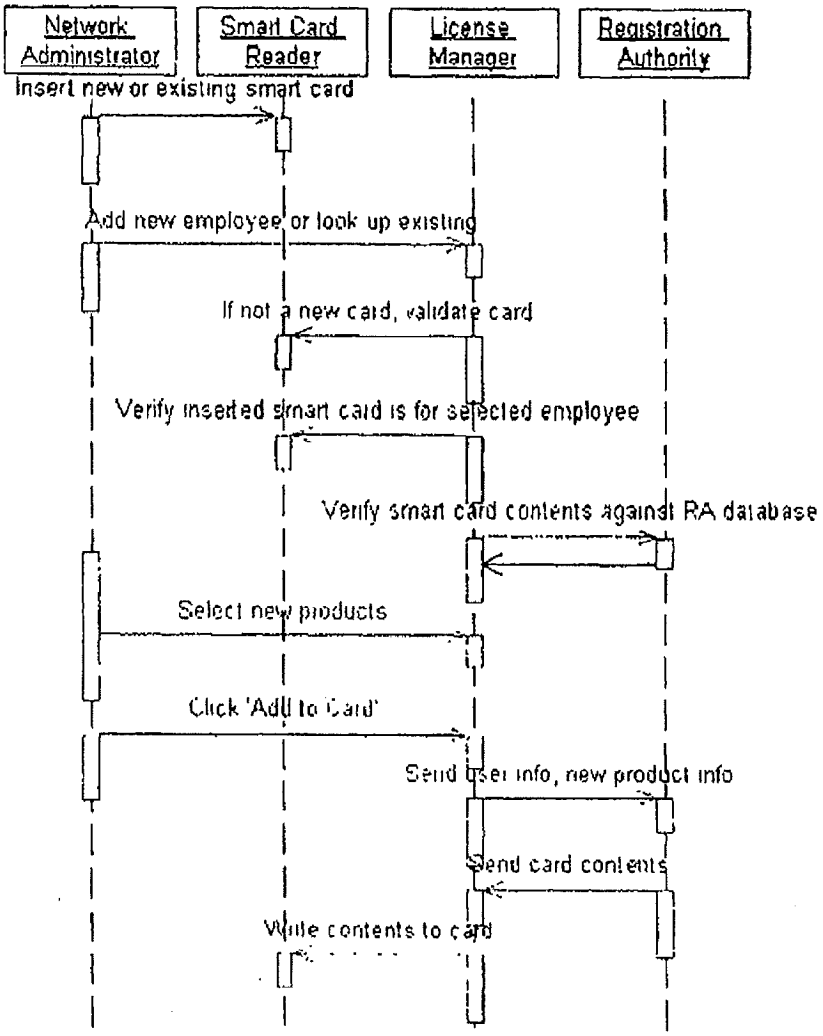

Network Administrator
Smart Card Reader
License Manager
Registration Authority
Insert new or existing smart card
Add new employee or look up existing
If not a new card, validate card
Verify inserted smart card is for selected employee
Verify smart card contents against RA database
Select new products
Click 'Add to Card'
Send user info, new product info
Send card contents
Write contents to card

Fig. 8

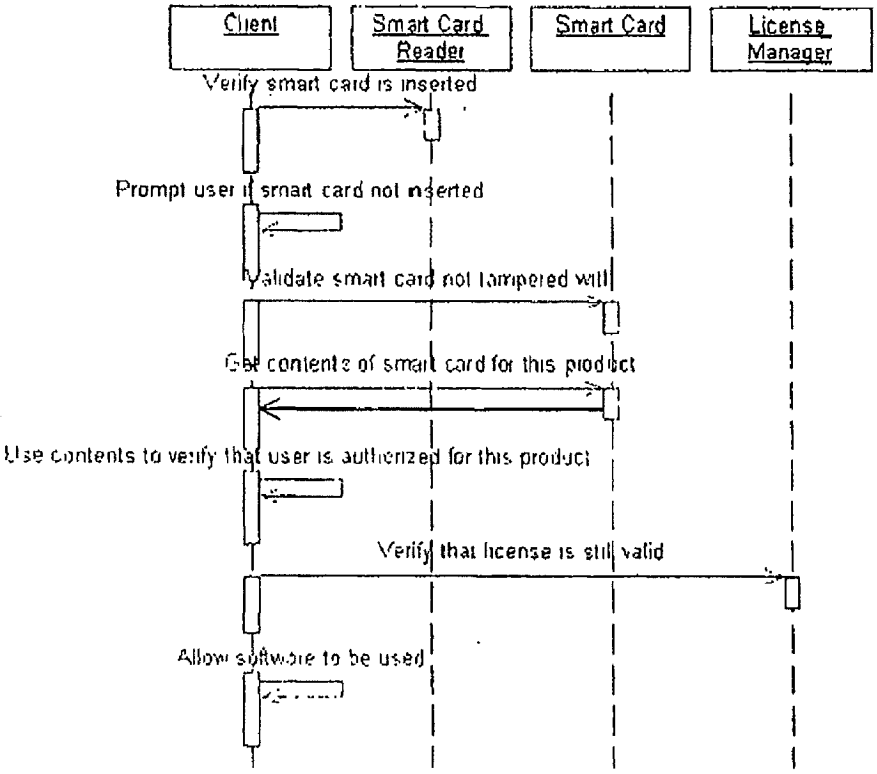

Client
Smart Card Reader
Smart Card
License Manager
Verify smart card is inserted
Prompt user if smart card not inserted
Validate smart card not tampered with
Get contents of smart card for this product
Use contents to verify that user is authorized for this product
Verify that license is still valid
Allow software to be used

Fig. 9

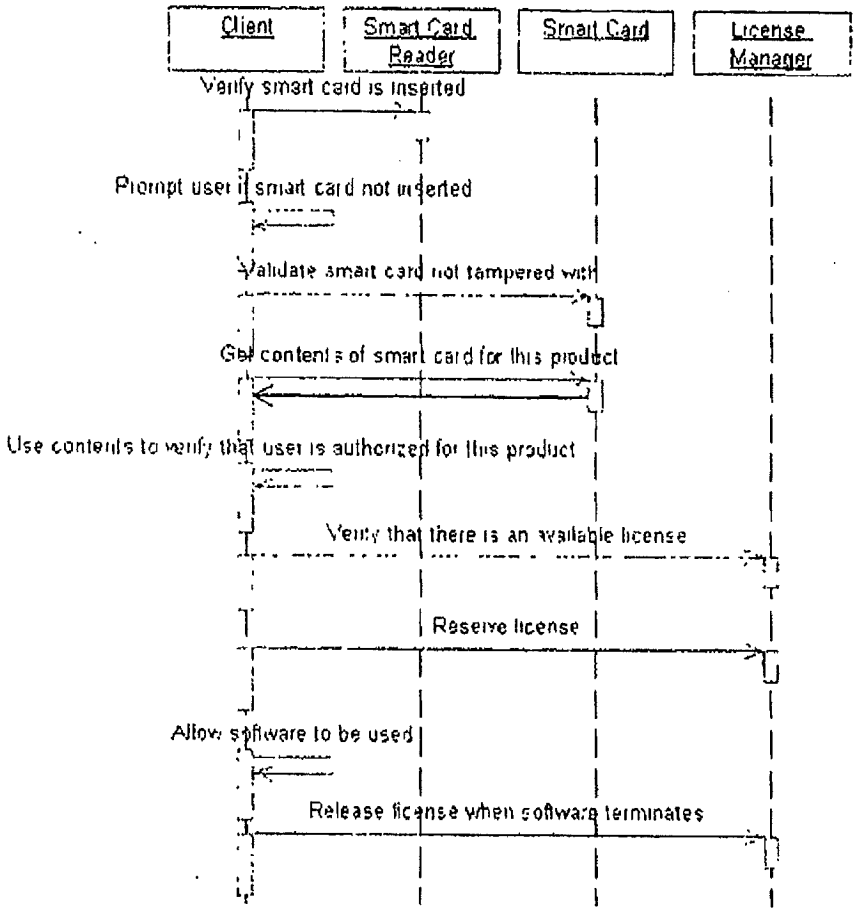

Client
Smart Card Reader
Smart Card
License Manager
Verify smart card is inserted
Prompt user if smart card not inserted
Validate smart card not tampered with
Get contents of smart card for this product
Use contents to verify that user is authorized for this product
Verify that there is an available license
Reserve license
Allow software to be used
Release license when software terminates

Fig. 10

SYSTEM AND METHOD FOR PREVENTING UNAUTHORIZED ACCESS TO ELECTRONIC DATA

This application claims the benefit of U.S. Provisional Application No. 60/229,934, filed Sep. 1, 2000.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to preventing unauthorized access to electronic data, such as for example computer software, music, movies, e-books, and the like. More specifically, the present invention relates to an access authorization system and method in which a client electronic device communicates with a licensing medium that stores license data identifying the electronic data to which the user is authorized to have access. The client electronic device also communicates with a central registration authority that contains a database used to verify the license data.

2. Related Art

Electronic devices, both wired and wireless, such as personal computers, handheld computing devices, personal data assistants, cellular telephones and CD and DVD players, are ubiquitous. These devices perform an increasing array of functions, including business, entertainment and educational type functions, just to name a few.

The common link between these electronic devices is their use of electronic data to perform their respective functions. The electronic data may be used to control the device itself, such as, for example, when the data comprise a computer software program. Alternatively, the electronic data may be intellectual content that is manipulated by these devices, such as, for example, when the data comprise music, movies, e-books, database information, or other forms of data that are privileged, copyrighted, proprietary or otherwise protected from unauthorized access.

In either case, the electronic data are valuable because of the time and effort that was expended in their creation. For example, a computer software program typically is the product of a labor-intensive development that involves software engineers, programmers, artists and marketers, just to name a few. Similarly, music, movies and e-books typically are the product of creative endeavors of artists and authors. In addition, the creation of all of these forms of electronic data may involve extremely costly production and marketing efforts.

By contrast, copying such electronic data typically requires very little time, effort and money. Consequently, unauthorized copying and distribution of electronic data is rampant. With regard to personal computer software, for example, it is estimated that 30% of software used in the United States is unlicensed and therefore unauthorized.

In certain foreign nations, in excess of 95% of the software programs in use are unauthorized copies, which were created in the United States or elsewhere and sold at a small fraction of their U.S. retail price. In some of these foreign nations, software piracy has become a large industry. This widespread unauthorized use of software and other electronic data has a potential chilling effect on the artists, entrepreneurs, and others who would create it.

The law, of course, provides some mechanisms for preventing or discouraging such piracy. Copyright protection, for example, is one of the most common legal means of protecting electronic data. Patent protection, also, is increasingly being used to protect some electronic data, particularly various aspects of computer software. Contractual provisions, such as licenses, are widely used as an adjunct to other forms of protection.

The right to use software under a license agreement may be restricted to a single user or a single computer. Where use on more than one computer is contemplated, such as in a local area network (LAN), the license may allow use on a number of computers. This sort of multiple computer license is often referred to as a site license, since it typically is implemented to allow several computers at a particular site to run the licensed software.

However, the effectiveness of these legal and contractual measures has been inadequate. Accordingly, vendors of electronic data have turned to technological means of protecting their intellectual content.

For example, licensed electronic data, such as computer software, may be protected from unauthorized use and/or copying by using a protection scheme that requires the user to register the licensed software with the vendor. Generally, such protection schemes use a registration program that is included with the software and executes upon installation of the software.

The registration program requires the user to enter a code sequence that was provided by the vendor with the software, e.g., printed on a CD-ROM case. The code sequence is checked by the registration program to determine whether it is valid. If it is valid, the registration program enables the user to use the software.

Conventional registration programs determine the validity of the code sequence using mathematical algorithms. Typically, such algorithms are simply the inverse of the algorithm initially used by the vendor to generate the set of valid code sequences that are distributed with the software.

While such conventional schemes do provide a rudimentary measure of security, they are far from unbeatable. In fact, such security systems are often thwarted by pirates who ascertain the algorithms for determining validity by analyzing the code sequences that they generate. Once an algorithm has been ascertained, it may be used by unauthorized users to generate valid code sequences for the licensed software. These valid code sequences or the algorithm itself, which is known as a keygen, then may be distributed widely to large numbers of unauthorized users. Indeed, keygens for many commercially successful licensed software products are freely available on the Internet.

Some vendors have attempted to improve upon the code sequence protection scheme by requiring users to enter certain personal information, such as the user's name and telephone number. This information is transmitted to the vendor where it is encoded and used in the code sequence generation process. The code sequence is sent back to the user, who uses it to unlock the software. However, this approach, like the code sequence approach discussed above, is also based on an ascertainable mathematical algorithm and therefore also may be circumvented for the same reason.

Another approach to preventing unauthorized access to licensed software is to require the user to have hardware keys, which are referred to as dongles, connected to the user's computer in order to use the licensed software. Typically, dongles are connected to the input/output (I/O) port of a computer.

There are numerous disadvantages in the use of dongles. For example, each piece of licensed software requires a separate dongle, but computers typically have a limited number of I/O ports. Consequently, a number of dongles may have to be connected to a single I/O port if several

pieces of license software are to be used. This may result in interference between the attached dongles, which may cause the dongles or the associated software to fail. Another disadvantage is that dongles may be easily lost or stolen. Software licensors typically replace lost or stolen dongles for a nominal fee, which may allow unauthorized users to easily obtain dongles.

Another approach to preventing unauthorized use and/or copying of licensed software is to require the user to have a licensing module connected to the user's network in order to use the licensed software. This approach is discussed in U.S. Pat. No. 6,101,606 (Diersch et al.). The module may contain an identification code and other licensing information. The licensed software periodically communicates with license management software on a network server. The license management software, in turn, communicates with the licensing module to determine whether a valid module is connected to the network.

There are several disadvantages to the licensing module approach. The licensing module contains a fixed identification code that may be ascertained through analysis of the module. Ascertaining the identification code would allow an unauthorized user to duplicate the module. Another disadvantage of the licensing module approach is that the licensing module is vulnerable to tampering. For example, a user may seek to increase the number of authorized users for a site licensing by changing licensing data stored in the module.

Yet another disadvantage of the licensing module approach is that authorized users are unable to use the licensed software on computers that are not connected to the single, fixed network. For example, an authorized user would not be able to use the licensed software on a laptop computer, personal digital assistant or other type of mobile computing device.

Another approach to preventing unauthorized use and/or copying of licensed software is to provide license management software that is installed on the user's server, as discussed in U.S. Pat. No. 6,049,789 (Frison et al.). The management software transmits pay-per-use license requests for the licensed software to a central license management system. The central license management system grants pay-per-use licenses to the user upon receiving these requests and maintains billing records.

This approach, however, suffers from the disadvantage that the user must be connected to the central license management system in order for a pay-per-use license to be granted. Consequently, as in the case of the licensing module, the software cannot be easily used on mobile electronic devices such as a laptop or personal data assistant.

There is a need, therefore, for a system and method for preventing unauthorized access to electronic data that takes an entirely fresh approach and overcomes the drawbacks of the conventional techniques.

SUMMARY OF THE INVENTION

The present invention generally provides a novel system and method for preventing unauthorized access to electronic data.

One aspect of the present invention provides a system and method for preventing unauthorized access to electronic data stored on an electronic device. A portable licensing medium is configured to communicate with the electronic device for storing license data. The license data is used by the electronic device to determine whether to allow access to the electronic data. A registration authority is configured to communicate with the electronic device. The registration authority has verification data for verifying the license data stored on the licensing medium. The registration authority provides updated license data to the licensing medium.

Embodiments of the present invention may include one or more of the following features. The electronic device may verify the validity of the licensing medium by comparing the license data to the verification data of the registration authority.

The licensing medium may store a license data message digest produced by performing a hash of the license data. The verification data may include a copy of the license data message digest. The electronic device may verify the validity of the licensing medium by comparing the license data message digest to the copy of the license data message digest in the verification data of the registration authority.

The license data message digest may be encrypted with a private key associated with the registration authority. The private key may be one of a number of private keys associated with the registration authority. The verification data may include a copy of the encrypted license data message digest. The electronic device may verify the validity of the licensing medium by comparing the encrypted license data message digest to the copy of the encrypted license data message digest in the verification data of the registration authority.

The electronic device may verify the validity of the licensing medium by decrypting the license data message digest read from the licensing medium using a public key associated with the registration authority, generating a message digest by performing a hash on the license data read from the licensing medium, and comparing the decrypted message digest to the generated message digest.

The electronic device may send registration information to the registration authority. The registration information may include a random identifier associated with the electronic data. The verification data stored in the registration authority database may include a list of authorized identifiers that allow access to the electronic data. The registration authority may provide updated license data to the licensing medium when the identifier sent with the registration information corresponds to one of the authorized identifiers.

The licensing medium may be a smart card having a memory. The smart card also may have a microprocessor. The smart card may decrypt a first message digest received from the registration authority using a public key associated with the registration authority, generate a second message digest by performing a hash on updated license data received from the registration authority, and compare the first message digest to the second message digest. The licensing medium may also be a memory stick, random access memory, or a computer disk (e.g., optical, magnetic, or electronic). The licensing medium may be a memory installed in a cellular telephone that may or may not be removable.

The license data may include a licensing medium expiration date determined by a configurable time period during which the licensing medium is valid. The licensing medium expiration period may be, e.g., thirty days.

The license data may include a software license expiration date determined by a configurable time period during which access to the electronic data is allowed. The software license expiration period may be, e.g., one day or thirty days.

The license data may include a software security expiration date determined by a configurable time period during which access to the electronic data is allowed. The software security expiration period may be, e.g., thirty days.

Another aspect of the present invention provides a system and method for preventing unauthorized access to electronic data stored on an electronic device. A portable licensing medium is configured to communicate with the electronic device for storing license data. The license data is used to determine whether to allow access to the electronic data. A registration authority is configured to communicate with the electronic device. The registration authority has a first database of verification data for verifying license data stored in a second verification database. A license manager is configured to communicate with the electronic device and the registration authority. The license manager has a second database of verification data for verifying the license data stored on the licensing medium. The license manager provides updated license data to the licensing medium.

Embodiments of the present invention may include one or more of the following features. The electronic device may verify the validity of the licensing medium by comparing the license data to the second database of verification data of the license manager. The license manager may verify the validity of the second database of verification data by comparing it to the first database of verification data of the registration authority.

The licensing medium may store a license data message digest produced by performing a hash of the license data. The second database of verification data may include a copy of the license data message digest. The electronic device may verify the validity of the licensing medium by comparing the license data message digest to the copy of the license data message digest in the second database of verification data of the license manager.

The license data message digest may be encrypted with a private key associated with the registration authority or the license manager. The private key may be one of a number of private keys associated with the registration authority or the license manager. The second database of verification data may include a copy of the encrypted license data message digest.

The electronic device may verify the validity of the licensing medium by comparing the encrypted license data message digest to the copy of the encrypted license data message digest in the second database of verification data of the license manager.

The electronic device may verify the validity of the licensing medium by decrypting the license data message digest read from the licensing medium using a public key associated with the registration authority, generating a message digest by performing a hash on the license data read from the licensing medium, and comparing the decrypted message digest to the generated message digest.

The license manager may send site license registration information to the registration authority. The site license registration information may include a random identifier associated with the electronic data. The verification data stored in the registration authority database may include a list of authorized identifiers that allow access to the electronic data. The registration authority may provide updated verification data to the license manager when the identifier sent with the registration information corresponds to one of the authorized identifiers.

The license manager may communicate with the registration authority to verify that the verification data stored by the license manager corresponds to the verification data stored by the registration authority.

These and other objects, features and advantages will be apparent from the following description of the preferred embodiments of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more readily understood from a detailed description of the preferred embodiments taken in conjunction with the following figures.

FIG. 1 is a block diagram of a system for protecting licensed electronic data used by a client computer.

FIG. 2 shows a smart card with surface contacts.

FIG. 3 is a block diagram of the internal microchip of the smart card.

FIG. 4 is a block diagram of a system for protecting licensed electronic data used by a remote client computer.

FIG. 5 is a block diagram of a system for protecting licensed electronic data used by a client computer network.

FIG. 6 is a diagram of software registration for a single-user system.

FIG. 7 is a diagram of software startup for a single-user system.

FIG. 8 is a diagram of adding a software license to an employee smart card in a multiple-user system.

FIG. 9 is a diagram of software startup for a fixed-node license in a multiple-user system.

FIG. 10 is a diagram of software startup for a floating license in a multiple-user system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG. 1 depicts a block diagram which illustrates in general terms an embodiment of the present invention. In FIG. 1, a personal computer **100**, referred to as the client device, may be configured to use licensed computer software provided by a third-party vendor.

Of course, the present invention is not limited to preventing unauthorized access to computer software on personal computers. Other examples of electronic devices that use licensed electronic data include DVD players, handheld computing devices, personal data assistants (PDAs), cellular or personal communication system (PCS) telephones, intelligent appliances (e.g., refrigerators and heating and cooling systems), internet appliances, etc. Other examples of licensed electronic data include computer software, music, movies, e-books, artwork, privileged data (such as databases, privileged publications and communications), etc. Still other examples of both exist as well.

In general terms, the protection system of the present invention uses a registration authority **110** that determines whether a given user is authorized to have access to a given piece of electronic data. As used herein, the phrase "access to electronic data" and its derivatives (e.g., "accessing electronic data") refers broadly to any type of manipulation of electronic data, including (but not limited to) installing, using, copying, inputting, outputting, reading, writing, deleting, viewing, playing, storing, moving, processing, etc. The registration authority **110** may be implemented as a server on a network, operated under the control of a software protection administrator. The software protection administrator maintains the registration authority **110** in cooperation the vendors of the electronic data.

As part of such a protection system, the vendor may require the user to install a client program provided by the software protection administrator. The client program installed on the client computer **100** communicates with a licensing information storage medium **120**, referred to as the licensing medium, and the registration authority **110**. Alternatively, the client program may be embedded in the

electronic data and may be executed in the course of accessing the electronic data, rather than being installed separately by the user. The registration authority **110**, in turn, communicates with the vendor **130**, which maintains a database of valid licenses issued for the electronic data.

The licensing medium **120** is a portable component that contains information concerning the software or other licensed electronic data that the user is authorized to access. When a user seeks to access a vended piece of electronic data, the client program communicates with the licensing medium **120** to verify that the user is authorized to access the electronic data.

In general, the licensing medium **120** may be any type of portable electronic data storage medium that has a unique, unalterable serial number or other form of identification that can be transmitted electronically. Examples include smart cards, memory sticks, magnetic strip cards, floppy disks and other removable computer storage media. The licensing medium **120** and the electronic device that uses the licensed electronic data need not have a wired connection. A wireless connection, e.g., an infrared or radio frequency (RF) link, may be used.

In certain types of electronic devices, the licensing medium **120** may be configured so that it is not removable, e.g., certain types of cellular phones, hand-held computing devices, or cable television control boxes. For example, the licensing medium may be an internal random access memory (RAM) installed in a cellular phone. It is also contemplated that the invention can include stationary devices, e.g., refrigerators or other household appliances, that have a licensing medium that is not removable.

In the example of FIG. **1**, a smart card is employed as the licensing medium. As shown in FIG. **2**, a smart card **120** is a plastic card containing a microchip **300**. Contacts **305** for the microchip **300** are formed on the surface of the card **120** to provide data input and output and power supply input.

As shown in FIG. **3**, the microchip **300** includes a central processing unit (CPU) **310** that has an associated random access memory (RAM) **315**, although a smart card without a CPU also may be used. The RAM **315** is used to temporarily store information during processing while power is being supplied to the card. A read only memory (ROM) **320** permanently stores the microchip operating system. An erasable programmable read only memory (EPROM) **325** stores application code and data, such as the licensing information discussed above.

Referring again to FIG. **1**, the client program accesses the smart card **120** using a smart card reader **140** connected to the client computer **100**. The smart card **120** contains licensing information that indicates to the client program which software the user is authorized to access. The licensing information may include other information as well, such as for example time-stamps that indicate when the license for each authorized software expires.

The smart card may be a dedicated smart card that is specifically provided for use as a licensing medium. Alternatively, a generic smart card having other functions, e.g., a credit card, may be adapted for use as the licensing medium. In such a case, the smart card would function both for the original purpose and as the licensing medium.

The registration authority **110** is a remote server that maintains a licensing database containing information for all of the licensing media **120** authorized by the software protection administrator and all of the software licenses authorized by the software vendors **130**. The client program communicates with the registration authority **110** to perform a number of functions associated with the operation of the protection system. The client program may communicate with the registration authority **110**, for example, using the Internet **150**.

For example, the client program may verify the validity of the smart card **120** by communicating with the registration authority **110**. As a further example, the client program communicates with the registration authority **110** to change the contents of the smart card **120** to add, remove, or modify the user's access to the software. The contents of the smart card **120** also may be changed in order to transfer a license to access the software from one smart card to another or to update time-stamps that indicate when authorization to use the software or the licensing medium itself expires.

As shown in FIG. **4**, the licensing medium and electronic device need not be co-located. For example, the licensing medium, e.g., a smart card **120**, may be connected to the user's computer **160**, which, in turn, is connected to the client device **100** through the Internet **150**. The client device **100** may be a remote server running licensed software or hosting a proprietary or commercial database that the user is authorized to access.

As a further example, the client device **100** may be a remote Internet web server containing computer aided drafting (CAD) files, such as building construction plans. In such a case, the smart card **120** effectively acts as a gatekeeper to allow authorized users, e.g., architects, builders, and contractors, to have access to the building plans.

As shown in FIG. **5**, the software may be licensed to the user pursuant to a site license, which allows a number of users at the license's location to use the software. A site license is typically purchased by a company that has a number of users connected to a local area network (LAN). In a site license configuration, the client program communicates with a licensing manager **200** provided on a server in the user's LAN. The licensing manager **200**, in turn, communicates with the registration authority **110** over the Internet **150**. A redundant licensing manager **210** may be provided for increased reliability.

In addition to the communication between the client program on the client computer **100** and the licensing medium **120** and registration authority **110** described above, the protection system also employs communication between the licensing medium **120** and the software.

The software includes application programming interfaces (APIs) that allow the software to periodically access the smart card to ensure that it is installed in the reader. The software also reads the licensing information contained on the smart card to ensure that the user's license is valid and has not expired or been revoked. If the software determines that the user does not have a valid license, then the software may suspend or halt operation, notify the user of the situation, give the user an opportunity to rectify the situation, and/or take other steps depending upon instructions included in the software by the vendor.

As discussed above, the user may be required to install a client program provided by the software protection administrator to install and register protected software. This may be done using an installation wizard provided by the software protection administrator, i.e., a program that controls the software installation process. The installation wizard may be included with the vendor's software on a compact disc read-only memory (CD-ROM), or it may already have been installed on the client computer during a prior software installation. The installation wizard installs the client program on the client computer.

Once the client program has been installed, the installation and registration of protected software proceeds as shown in FIG. 6. The protected software is installed on the client computer, and the user is prompted to register the installed software with the registration authority.

To register the software, the user must insert a smart card into a reader connected to the computer and must have an Internet connection or modem. If these means of connection are not present or if the user does not want to register the software at the time of installation, the user may be permitted to use the software for a limited time in a trial mode in accordance with the vendor's licensing policies.

The client program reads the data from the smart card and transmits it to the registration authority along with a set of registration information. The registration authority first compares the smart card data to corresponding data stored in a database to verify that the smart card is valid. The registration authority then compares the registration information to corresponding data stored in a database to verify that the new software registration is authorized.

The smart card data sent to the registration authority includes a message digest that was generated by a performing a hash function on the smart card data. A hash function takes a data stream of arbitrary length and generates a fixed-length code, which is referred to as the message digest or hash. The registration authority compares the message digest to a corresponding entry in the database to verify that the smart card is valid.

Hash functions having the following properties are generally considered to be cryptographically suitable, i.e., secure. First, the hash function must be essentially a one-way function, so that given a message digest, it is nearly impossible to determine the original data stream. Second, the hash function must produce virtually unique message digests, so that it is nearly impossible to find two messages that produce the same message digest. Commonly used hash functions include: Message Digest 2 (MD2), Message Digest 4 (MD4), Message Digest 5 (MD5), the Secure Hash Algorithm (SHA), and the Secure Hash Algorithm 2 (SHA-2).

The registration information sent to the registration authority includes the unique identifier of the software to be registered. The identifier may be composed of a serial number and a password or passphrase to prevent an unauthorized user from guessing serial numbers. The serial number and password are printed on the CD-ROM case in which the software is distributed. Alternatively, the identifier may be generated from two unrelated components, e.g., two words randomly selected from the dictionary. The registration authority compares the identifier received with the registration information to a database of valid identifiers provided by the software vendor.

The registration information sent to the registration authority also includes other information, such as a product number for the software to be registered, a unique smart card serial number, a smart card sequence number. The registration information also includes expiration periods for the smart card and the software licenses, as further discussed below.

If the registration information is verified by the registration authority, then a new registration entry is created for the newly granted or updated license for the software. The registration authority generates new smart card data reflecting these changes and sends the new data back to the client computer to be stored on the smart card.

The registration authority also sends a hash of the new smart card data to the client computer. The hash is encrypted with a private key belonging to the software protection administrator. The encrypted hash may be decrypted by anyone having a corresponding public key. However, only the software protection administrator can generate such an encrypted hash. In effect, the encrypted hash becomes a digital signature of the software protection administrator.

The private key used by the software protection administrator may be one of a set of private keys, e.g., a set of 100 keys. Using a large set of private keys makes cracking any particular key in the set more difficult, since a different key may be used for each update.

The client program receives the new data and encrypted hash and stores it on the smart card. Each time the smart card is accessed in this manner, the smart card performs a hash comparison using its internal processor to prevent unauthorized changes to the smart card data.

To perform the hash comparison, the smart card processor decrypts the hash received from the registration authority using a public key. The smart card then generates a hash for the new data. The generated hash and the decrypted hash are compared to ensure that the new data came from the registration authority.

The new smart card data sent by the registration authority also includes a new smart card sequence number, a new expiration date for the smart card, software license expiration dates, and software security expiration dates.

The smart card sequence number allows the registration authority to track updates to the smart card. For example, the sequence number may be an n-bit (where n is an integer) word that is incremented each time the smart card is updated. This feature allows the registration authority to detect unauthorized access to the smart card.

The software license expiration date is determined by a configurable time period during which the license is valid based on the license agreement with the user. For example, the software license expiration period may be one hour, one day, thirty days, one year, or any agreed upon period of time.

Each software license may have a corresponding software security expiration date that is determined by a configurable time period within which the user must reconnect to the registration authority to renew the software license. The software security expiration period may be determined by the vendor based on security considerations and may be any desired length of time.

The smart card expiration date is determined by configurable time period during which the smart card will operate. The smart card expiration period may be determined by the software protection administrator based on security or other considerations and may be any desired length of time, e.g., 30 days. The smart card expiration period may be set to be equal to the shortest software security expiration period stored on the card.

The smart card must be updated by the registration authority within the smart card expiration and software security expiration periods for the user to have uninterrupted use of the software. Consequently, if a smart card were lost or stolen, an unauthorized user would only be able to use the smart card for the remainder of the shortest of these expiration periods. In addition, the lost or stolen smart card can be disabled the next time the electronic device communicates with the registration authority.

The new smart card data sent by the registration authority may include an authorization key for the software, for example, a hash of the product expiration date and product number. The authorization key indicates to the smart card

that the user is authorized to use the software. Alternatively, if storage space or time are at a premium, a binary flag may be used as an authorization key.

As discussed above, the new data stored on the smart card allows the user to use the software for a configurable time period, e.g., 30 days, as indicated by the software license and software security expiration dates. The software can be used during these time periods without further communication with the registration authority, provided the smart card is present.

The software license expiration period may be used to implement a short term license. For example, a software license may be purchased on a daily basis. In such a case, the user would leave the software installed on the user's computer, but would connect with the registration authority only when the software was needed. Upon connecting to the registration authority, the user would receive new smart card data, which would have a software license expiration period of one day.

To remove a registered software product from a smart card, the user may run a removal program, e.g., a Windows™ control panel applet. The removal program connects to the registration authority, which modifies the database of authorized software licenses. The serial number of the removed software may be returned to a database of authorized serial numbers so that another user may register it, or the serial number may be placed in an inactive status until it is reactivated.

The registration authority sends new smart card data to the user reflecting the removal of the software license. Rather than deleting the entry on the smart card, the registration authority may change the software license expiration date to a date in the past. Consequently, the smart card data would indicate that the product had been licensed to the smart card, but was no longer valid.

During the software registration process, the user will be asked whether to allow automatic updating of the smart card data whenever an Internet connection is detected. If the user allows automatic updates, then a software module, such as a daemon (i.e., a process that runs in the background and performs a specified operation at predefined times or in response to certain events), may be used to continuously monitor for an Internet connection and update the smart card data in the background. Alternatively, a background task initiated by the client program may perform these functions in a manner similar to the Microsoft Critical Update Manager. Automatic updating of the smart card data would allow the user to maintain the maximum software license expiration period, e.g., thirty days, on all of the licensed software.

During an automatic update of the smart card, the smart card data, including the encrypted hash of the smart card data and the sequence number, are transmitted to the registration authority. The smart card data also includes any registered products that have been added to the card since the last update, such as trial use installations. The new product entries also may include new software installations in which the vendor allows temporary registration without connecting to the registration authority. The presence of new products on the smart card may be detected by examining a last-registered field stored on the smart card or a binary field for each registered product.

Upon receiving the smart card data, the registration authority checks a database of verification data to verify that the smart card data is valid. The database may be, for example, a logical database that is stored separately or with other data in another logical or physical database. The registration authority verifies such items as the smart card sequence number and the smart card expiration date. In addition, the encrypted hash of the smart card data is verified by decrypting it using a public key.

Following the verification of the smart card data, the registration authority stores the new smart card data in its database. The registration authority generates new smart card data to update the expiration date and sequence number of the smart card and generates a new encrypted hash of this new smart card data. The new smart card data is stored on the card and an acknowledgement is sent to the registration authority.

As discussed above, if the user does not have an Internet connection or modem or does not want to register the software at the time of installation, the user may be permitted to use the software for a limited time in a trial mode in accordance with the vendor's licensing policy.

If the vendor licensing policy permits trial use, then the client program will be configured to establish a trial use for the user. The client program first checks the installed smart card to determine whether there already is a trial entry for the software in question. A trial entry is made on the smart card when a user is first granted a trial use for the software and is stored on the smart card indefinitely. Accordingly, the client program can determine whether the user has previously been granted a trial use and, if so, the client program may not grant successive trial uses.

When a trial entry is made, a new hash is performed on the new smart card data including the trial entry and stored on the smart card. Consequently, the trial entry cannot be deleted without invalidating the smart card.

If the user has not previously been granted a trial for the software, a trial entry is made on the smart card. The trial entry includes a configurable time limit for the trial use, e.g., 30 days. The user may then use the software for the trial period.

If the user later has access to an internet connection, the trial version may be converted to a full license if the appropriate registration procedures are performed or the registration authority has received authorization from the vendor. As discussed above, the software also may be configured to ask the user whether an automatic upgrade is desired upon detection of an internet connection.

To use the registered software, the user must insert a smart card containing valid license information into the smart card reader of the client computer, i.e., a smart card that has been prepared as described above. As shown in FIG. 7, when the user attempts to activate the software, the client computer checks to see whether a smart card is inserted. If not, the user is prompted to insert the smart card.

The client program reads the contents of the smart card and verifies that it has not been tampered with. The client program then retrieves the licensing information for the particular software. The licensing information allows the client program to determine whether the user is authorized to use the software and that the authorized period of use or trial use has not expired.

The client program may use the encrypted hash to detect whether the smart card has been altered. The client program decrypts the message digest stored on the smart card using a public key. The client program then generates a message digest for the smart card data using a hash function. The client program then compares the generated message digest to the decrypted message digest. If these message digests agree, then the smart card has not been altered. This procedure allows the client program to verify the validity of the smart card without communicating with the registration authority.

Once the verification has been completed, the client program allows the software to be used. During use, the software periodically checks for the presence of a valid smart card using application programming interfaces (APIs) at intervals determined by the software vendor. The APIs are provided by the software protection administrator and may be implemented as dynamically linked libraries (DLLs).

To prevent tampering, the DLLs may be signed so that they can be validated. If it is determined that modules have been tampered with, the software will stop functioning until such modules have been replaced.

Time stamps may be stored on the smart card when it is checked by the APIs. The time stamps are used to prevent a user from resetting the system clock to maintain registration beyond the software license expiration date.

Referring again to FIG. **5**, a site license may be purchased by a company to allow software to be used by multiple users on a LAN. The number of users is determined at the time of purchase. The site-license-holder LAN includes a license manager **200**, which may also be the server for the LAN.

The license manager **200** acts as an intermediary between the client computers **100** and the registration authority **110**. For example, the license manager **200** communicates with the registration authority **110** to register the site license. Typically, the vendor **130** of the site license has transmitted information regarding a new site license to the registration authority **110** prior to registration. The license manager **200** registers the site license by transmitting to the registration authority **110** the serial number/password supplied with the software.

Alternatively, registration may proceed in a manner similar to the single user installation described above. In such a case, the company's license administrator, who is usually the LAN administrator, installs the site-licensed software. An installation wizard installs a license management program that verifies the validity of the inserted smart card **120**. The license management program also communicates with the registration authority **110** to verify the contents of the smart card **120** and register the site license.

The license manager **120** maintains a database of all of the site-licensed software installed on the LAN. The site license database is synchronized periodically with a corresponding database at the registration authority **110**. The site license database includes information regarding the number of fixed node and floating licenses.

Fixed node licenses are assigned to particular individuals, e.g., an employee of the company that holds the site license. Once the fixed node license is assigned, there is one less license available to the company. The license manager maintains entries in the site license database for each of the assigned fixed node licenses.

Floating licenses allow a fixed number of employees to concurrently use the software. If a employee discontinues use of the software, an additional license becomes available to other employees. The license manager continuously maintains a list of current users to ensure that the number of concurrent users does not exceed the total number of floating licenses.

As described above, the license manager 200 communicates with the registration authority **110** to register the site-licensed software and maintains the site license database. In addition, as shown in FIG. **8**, the license manager is used by the company's license administrator to create and modify smart cards that are issued to each employee. The smart cards are programmed with encrypted licensing information indicating which site-licensed software the employee is authorized to access.

The license administrator inserts a new or existing smart card **120** into a smart card reader **140** connected to the license administrator's computer **100**, which is connected to the LAN server/License manager **200**. The license administrator's computer **100** communicates with the license manager **200** to look up the corresponding stored data or add a new entry.

If the smart card **120** is for a selected existing employee, the license manager **200** will verify the contents of the smart card **120** and verify that the smart card **120** belongs to the selected employee. The license manager **200** then communicates with the registration authority **110** to verify the validity of the smart card **120** using corresponding data stored in the registration authority database.

Once the validity of the smart card **120** has been verified, the license administrator may select new licenses from the available site licenses to add to the employee's card **120**. The license manager **200** generates new licensing information for the smart card **120** and transmits it to the registration authority **110**. The registration authority 110 sends back new contents for the smart card **120**, which are written on the card **120** by the smart card reader **140**.

To use the registered software, the user must insert a smart card **120** containing valid license information into the smart card reader **140** of the client computer **100**, i.e., a smart card that has been prepared as described above. As shown in FIG. **9**, when a user having a fixed-node site license attempts to activate the software, the client computer **100** checks to see whether a smart card **120** is inserted. If not, the user is prompted to insert the smart card **120**.

The client program on the client computer **100** reads and verifies the validity of the smart card 120 to ensure that it has not been tampered with. The verification process is described in further detail below. The client program then retrieves the licensing information for the particular software. The licensing information allows the client program to verify that the user is authorized to use the software and that the authorized period of use or trial use has not expired.

The client program on the client computer **100** then communicates with the license manager 200 to verify that the user has a valid fixed-node license. If the user does not have a fixed-node license entry in the site license database stored by the license manager 200, the license manager 200 may check for an available floating license, as discussed in further detail below. If neither a fixed-node nor floating license is available, the user will not be verified. This configuration allows the license manager **200** to control the assignment of fixed-node licenses without connecting to the registration authority **110**.

Once the verification has been completed, the client program allows the software to be used. During use, the software may periodically reverify the smart card using APIs at intervals determined by the software vendor.

Similarly, as shown in FIG. **10**, when a user having a floating site license attempts to activate the software, the client computer 100 checks to see whether a smart card 120 is inserted. If not, the user is prompted to insert the smart card 120.

The client program on the client computer 100 reads and verifies the validity of the contents of the smart card 120 to ensure that it has not been tampered with. The client program then retrieves the licensing information for the particular software.

The client program on the client computer **100** then communicates with the license manager **200** to determine whether a floating license is available. If a floating license is

available, it will be reserved for the user, i.e., the number of available licenses will be decreased by one. This configuration allows the license manager 200 to control the assignment of floating licenses without connecting to the registration authority 110.

Once the verification has been completed, the client program allows the software to be used. During use, the software may periodically reverify the smart card using APIs at intervals determined by the software vendor. When the user terminates the software, the client computer will allow the license manager to release the floating license to other users.

An employee may wish to use registered software on a computer that is not connected to the LAN, e.g., a laptop or home computer. In such a case, the client program would not be able to communicate with the license manager to verify that the user has a valid fixed-node license or that a floating license is available, as discussed above. The employee's smart card therefore must be modified by the license manager to allow offsite use of the registered software.

For a fixed-node license, the license manager creates an entry on the employee's smart card that allows use of the software for a license period, e.g., 30 days. During this period, the employee may use the software without connecting to the license manager for verification.

For a floating license, the license manager creates an entry on the employee's smart card that allows use of the software for a license period, e.g., 30 days, and reserves a floating license. During this period, the employee may use the software without connecting to the license manager for verification. However, other employees will not be able to access the reserved floating license during this period regardless of whether the floating license is actually being used by the off-site employee.

The employee may connect to the LAN while off-site, for example, to check for email. Upon connecting to the LAN, the license manager may automatically update the employee's smart card to restart the license period. Hence, if an employee checks more frequently than the license period, the software may be used off-site indefinitely.

When a user acquires a new smart card, it must be registered with the registration authority before licensing information is stored on it. The registration is done using a registration wizard installed on the client computer.

The registration wizard may be installed automatically during installation of the first protected software product in a manner similar to the installation of the client program discussed above. Alternatively, the registration wizard may be downloaded from the Internet, bundled with a smart card reader, or included in the operating system.

During registration of the smart card, the registration wizard prompts the user to enter a number of questions and answers that most likely are known only to the user. These questions and answers are encrypted using a private key and sent to the registration authority along with the card serial number. This information may be used during software registration and use to verify that the user is the actual owner of the smart card.

The smart card serial number may be stored on the client computer, e.g., in the registry. If the user forgets or loses the serial number, the user can run an applet to retrieve smart card serial numbers from the registry. The applet also may indicate the software products that are registered on the smart card.

The user will be instructed to keep the smart card serial number in a safe place to facilitate replacement if the card is lost, damaged, or stolen. If the user does not known the serial number of the smart card or does not have access to the client computer, the user may contact the vendor of one of the software products licensed to the smart card. The vendor can provide the serial number of the software, which can be used by the registration authority to look up the smart card serial number.

If a smart card is lost, damaged, or stolen, the user may call a toll-free number or use the Internet to submit the necessary information to the registration authority or the vendor to have the licenses stored on the old card, including trial licenses, transferred to a new card. The old card then is disabled in the registration authority database.

If an unauthorized user attempts to renew licenses on the old smart card by connecting to the registration authority, the old smart card will be disabled. If it is determined that the old smart card was issued recently, the licensing period for the software products may be shortened on the new smart card to prevent repeated smart card replacement.

It will be appreciated that each of these embodiments discussed above provides a novel system and method for preventing unauthorized access to electronic data that achieves the above discussed objects of the present invention.

It also will be appreciated that because the licensing medium can include licenses from multiple vendors, the system enables a user to access data from multiple vendors without the need for multiple keys or access devices.

It also will be appreciated that because the licensing medium is associated with a particular user, rather than a particular electronic device, the user can access the licensed electronic data using a number of different electronic devices, e.g., on a home computer and a laptop.

It also will be appreciated that because the licensing medium can store license data for electronic data from a number of vendors, the user may conveniently access all of the data for which the user is licensed using a single licensing medium.

It also will be appreciated that because the licensing medium is portable, the system may be used on any computer capable of reading the licensing medium. Hence, the protected electronic data may be accessed by the holder of the licensing medium on a home computer, laptop computer, handheld computer, etc.

It also will be appreciated that because the licensing medium permits access to the protected electronic data for a configurable time period, the user may access the data without connecting to the registration authority during the time period. Consequently, a fixed connection to the registration authority or the Internet is not required.

It also will be appreciated that because the licensing medium permits access to the protected electronic data for a configurable time period, the vendor may offer short term licenses, e.g., weekly, daily, hourly, etc.

It will also be appreciated that because a smart card has an internal processor, it can perform encryption, decryption, and hash functions. Consequently, the smart card can decrypt a received hash and compare it to an internally generated hash of the smart card data. This comparison allows the smart card to determine whether new data received is from an authorized source and thereby prevent unauthorized modification of the smart card data.

While the present invention has been described with respect to what is presently considered to be the preferred embodiments, it is to be understood that the invention is not

limited to the disclosed embodiments. To the contrary, the invention is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

What is claimed:

1. A system for preventing unauthorized access to electronic data on an electronic device, the system comprising:

a portable licensing medium configured to communicate with the electronic device and to store license data, the license data configured to be used by the electronic device to determine whether to allow access to the electronic data; and

a registration authority configured to communicate with the electronic device, the registration authority having verification data for verifying the license data stored on the licensing medium,

wherein the registration authority provides updated license data for the licensing medium.

2. A system according to claim 1, wherein the electronic device is configured to verify validity of the licensing medium by comparing the license data to the verification data.

3. A system according to claim 1, wherein the licensing medium is configured to store a license data message digest produced by performing a hash of the license data.

4. A system according to claim 3, wherein the verification data comprises a copy of the license data message digest.

5. A system according to claim 4, wherein the electronic device is configured to verify validity of the licensing medium by comparing the license data message digest to the copy of the license data message digest in the verification data.

6. A system according to claim 3, wherein the license data message digest is encrypted with a private key associated with the registration authority.

7. A system according to claim 6, wherein the private key is one of a plurality of private keys associated with the registration authority.

8. A system according to claim 6, wherein the verification data comprises a copy of the encrypted license data message digest.

9. A system according to claim 8, wherein the electronic device is configured to verify validity of the licensing medium by comparing the encrypted license data message digest to the copy of the encrypted license data message digest in the verification data.

10. A system according to claim 6, wherein the electronic device is configured to verify validity of the licensing medium by:

decrypting the license data message digest read from the licensing medium using a public key associated with the registration authority;

generating a message digest by performing a hash on the license data read from the licensing medium; and

comparing the decrypted message digest to the generated message digest.

11. A system according to claim 1, wherein the electronic device is configured to send registration information to the registration authority.

12. A system according to claim 11, wherein the registration information comprises a random identifier associated with the electronic data.

13. A system according to claim 12, wherein the verification data comprises a list of authorized identifiers that allow access to the electronic data.

14. A system according to claim 13, wherein the registration authority is configured to provide updated license data to the licensing medium when the identifier sent with the registration information corresponds to one of the authorized identifiers.

15. A system according to claim 1, wherein the licensing medium comprises a smart card having a memory.

16. A system according to claim 15, wherein the smart card has a microprocessor.

17. A system according to claim 15, wherein the smart card is configured to decrypt a first message digest received from the registration authority using a public key associated with the registration authority, to generate a second message digest by performing a hash on updated license data received from the registration authority, and to compare the first message digest to the second message digest.

18. A system according to claim 15, wherein the license data comprises a sequence number that allows the registration authority a number of times the smart card has been accessed.

19. A system according to claim 1, wherein the licensing medium is a memory stick.

20. A system according to claim 1, wherein the licensing medium is a random access memory.

21. A system according to claim 1, wherein the licensing medium comprises a memory installed in a cellular telephone.

22. A system according to claim 21, wherein the licensing medium is not removable from the cellular telephone.

23. A system according to claim 1, wherein the licensing medium is a computer disk.

24. A system according to claim 23, wherein the computer disk is an optical disk.

25. A system according to claim 23, wherein the computer disk is a magnetic disk.

26. A system according to claim 23, wherein the computer disk is an electronic disk.

27. A system according to claim 1, wherein the license data comprises a licensing medium expiration date determined by a configurable time period during which the licensing medium is valid.

28. A system according to claim 1, wherein the license data comprises a software license expiration date determined by a configurable time period during which access to the electronic data is allowed.

29. A system according to claims 27 or 28, wherein the licensing medium expiration period is set to a shortest software license expiration period of the license data.

30. A system according to claim 1, wherein the license data comprises a software security expiration date determined by a configurable time period during which access to the electronic data is allowed.

31. A system according to claim 1, wherein the licensing medium is configured to communicate with the electronic device through a wired connection.

32. A system according to claim 1, wherein the licensing medium is configured to communicate with the electronic device through a wireless connection.

33. A system according to claim 1, wherein the licensing medium is configured to communicate with the electronic device through a network.

34. A system according to claim 33, wherein the network is the Internet.

35. A system for preventing unauthorized access to electronic data on an electronic device, the system comprising:

license data storage means configured to communicate with the electronic device, the license data configured to be used by the electronic device to determine whether to allow access to the electronic data; and

registration authorization means configured to communicate with the electronic device, the registration authorization means having verification means for verifying the license data stored on the licensing medium,

wherein the registration authorization means is configured to provide updated license data to the license data storage means.

36. A system for preventing unauthorized access to electronic data on an electronic device, the system comprising:

a smart card configured to communicate with the electronic device and configured to store license data, the license data configured to be used by the electronic device to determine whether to allow access to the electronic data; and

a registration server configured to communicate with the electronic device, the registration server having verification data for verifying the license data stored on the smart card,

wherein the registration server is configured to provide updated license data to the smart card.

37. A registration authority for preventing unauthorized access to electronic data on an electronic device, the registration authority comprising:

means for communicating with the electronic device; and

verification data for verifying license data stored on a portable licensing medium that is configured to communicate with the electronic device,

wherein the license data is used by the electronic device to determine whether to allow access to the electronic data, and

the registration authority is configured to provide updated license data to the licensing medium.

38. A smart card for preventing unauthorized access to electronic data on an electronic device, the smart card comprising:

means for communicating with the electronic device;

a memory for storing data received from the communicating means; and

license data stored in the memory, the license data being configured to be used by the electronic device to determine whether to allow access to the electronic data,

wherein the license data has been verified by verification data stored on a registration server that is configured to communicate to the electronic device, and

the smart card is configured to receive provide updated license data from the registration server.

39. A system for preventing unauthorized access to electronic data on an electronic device, the system comprising:

a portable licensing medium configured to communicate with the electronic device and configured to store license data, the license data is configured to be used to determine whether to allow access to the electronic data;

a registration authority having a first verification database for verifying license data stored in a second verification database; and

a license manager configured to communicate with the electronic device and the registration authority, the license manager having the second verification database for verifying the license data stored on the licensing medium,

wherein the registration authority is configured to provide updated verification data for the second verification database of the license manager, and

the license manager is configured to provide updated license data to the licensing medium.

40. A system according to claim 39, wherein the electronic device is configured to verify validity of the licensing medium by comparing the license data to the second verification database.

41. A system according to claim 39, wherein the license manager is configured to verify validity of the second verification database by comparing it to the first verification database.

42. A system according to claim 39, wherein the licensing medium is configured to store a license data message digest produced by performing a hash of the license data.

43. A system according to claim 42, wherein the second verification database comprises a copy of the license data message digest.

44. A system according to claim 43, wherein the electronic device is configured to verify validity of the licensing medium by comparing the license data message digest to the copy of the license data message digest in the second verification database.

45. A system according to claim 42, wherein the license data message digest is encrypted with a private key associated with the registration authority or the license manager.

46. A system according to claim 45, wherein the private key is one of a plurality of private keys associated with the registration authority or the license manager.

47. A system according to claim 45, wherein the second verification database comprises a copy of the encrypted license data message digest.

48. A system according to claim 47, wherein the electronic device is configured to verify validity of the licensing medium by comparing the encrypted license data message digest to the copy of the encrypted license data message digest in the second verification database.

49. A system according to claim 47, wherein the electronic device is configured to verify validity of the licensing medium by:

decrypting the license data message digest read from the licensing medium using a public key associated with the registration authority;

generating a message digest by performing a hash on the license data read from the licensing medium; and

comparing the decrypted message digest to the generated message digest.

50. A system according to claim 39, wherein the license manager is configured to send site license registration information to the registration authority.

51. A system according to claim 50, wherein the site license registration information comprises a random identifier associated with the electronic data.

52. A system according to claim 51, wherein the first verification database comprises a list of authorized identifiers that allow access to the electronic data.

53. A system according to claim 52, wherein the registration authority is configured to provide updated verification data to the license manager when the identifier sent with the registration information corresponds to one of the authorized identifiers.

54. A system according to claim 39, wherein the license manager is configured to communicate with the registration authority to verify that the second verification database corresponds to the first verification database.

55. A system according to claim 39, wherein the license data comprises a licensing medium expiration date determined by a configurable time period during which the licensing medium is valid.

56. A system according to claim 39, wherein the license data comprises a software license expiration date determined by a configurable time period during which access to the electronic data is allowed.

57. A system according to claims 55 and 56, wherein the licensing medium expiration period is set to a shortest software license expiration period of the license data.

58. A system according to claim 39, wherein the license data comprises a software security expiration date determined by a configurable time period during which access to the electronic data is allowed.

59. A system according to claim 39, wherein the licensing medium is configured to communicate with the electronic device through a wired connection.

60. A system according to claim 39, wherein the licensing medium is configured to communicate with the electronic device through a wireless connection.

61. A system according to claim 39, wherein the licensing medium is configured to communicate with the electronic device through a network.

62. A system according to claim 61, wherein the network is the Internet.

63. A system for preventing unauthorized access to electronic data on an electronic device, the system comprising:

license data storage means configured to communicate with the electronic device, the license data being used to determine whether to allow access to the electronic data;

registration authorization means having a first verification means for verifying license data provided by a second verification means; and

license management means configured to communicate with the electronic device and the registration authorization means, the license management means having the second verification means for verifying the license data stored on the license data storage means,

wherein the registration authorization means is configured to provide updated verification data for the second verification database of the license management means, and

the license management means is configured to provide updated license data to the license data storage means.

64. A system for preventing unauthorized access to electronic data on an electronic device, the system comprising:

a smart card configured to communicate with the electronic device and configured to store license data, the license data being used to determine whether to allow access to the electronic data;

a registration server having a first verification database for verifying license data stored in a second verification database; and

a license management server configured to communicate with the electronic device and the registration server, the license management server having the second verification database for verifying the license data stored on the smart card,

wherein the registration server is configured to provide updated verification data for the second verification database of the license manager server, and

the license management server is configured to provide updated license data to the smart card.

65. A registration authority for preventing unauthorized access to electronic data on an electronic device, the registration authority comprising:

means for communicating with the license manager; and

a first verification database for verifying license data stored in a second verification database on a license manager that is configured to communicate with the electronic device,

wherein the second verification database is configured to verify license data stored on a portable licensing medium that is configured to communicate with the electronic device,

the license data is configured to be used to determine whether to allow access to the electronic data, and

the registration authority is configured to provide updated verification data to the second verification database of the license manager.

66. A smart card for preventing unauthorized access to electronic data on an electronic device, the smart card comprising:

means for communicating with the electronic device;

a memory for storing data received from the communicating means; and

license data stored in the memory, the license data being configured to be used by the electronic device to determine whether to allow access to the electronic data,

wherein the license data has been verified by a license management verification database stored on a license management server configured to communicate with the electronic device and a registration server, and the license management verification database has been verified by a registration database stored on the registration server, and

the smart card is configured to receive updated license data from the license management server.

67. A method for preventing unauthorized access to electronic data stored on an electronic device, the method comprising the steps of:

storing license data on a portable licensing medium configured to communicate with the electronic device;

determining whether to allow access to the electronic data based on the license data;

verifying the license data stored on the licensing medium using a registration authority having verification data and being configured to communicate with the electronic device; and

providing updated license data to the licensing medium using the registration authority.

68. A method according to claim 67, wherein during the verifying step, the electronic device compares the license data stored on the licensing medium to the verification data.

69. A method according to claim 67, wherein the licensing medium stores a license data message digest produced by performing a hash of the license data.

70. A method according to claim 69, wherein the verification data comprises a copy of the license data message digest.

71. A method according to claim 70, wherein in the verifying step, the electronic device compares the license data message digest stored on the licensing medium to the copy of the license data message digest in the verification data.

72. A method according to claim 69, wherein the license data message digest is encrypted with a private key associated with the registration authority.

73. A method according to claim 72, wherein the private key is one of a plurality of private keys associated with the registration authority.

74. A method according to claim 72, wherein the verification data comprises a copy of the encrypted license data message digest.

75. A method according to claim 74, wherein in the verifying step, the electronic device compares the encrypted license data message digest stored on the licensing medium to the copy of the encrypted license data message digest in the verification data.

76. A method according to claim 72, further comprising the steps of:

reading the encrypted license data message digest from the licensing medium using the electronic device;

decrypting the license data message digest using a public key associated with the registration authority;

generating a message digest by performing a hash on the license data read from the licensing medium; and

comparing the decrypted message digest to the generated message digest.

77. A method according to claim 67, further comprising the step of sending registration information to the registration authority using the electronic device.

78. A method according to claim 77, wherein the registration information comprises a random identifier associated with the electronic data.

79. A method according to claim 78, wherein the verification data comprises a list of authorized identifiers that allow access to the electronic data.

80. A method according to claim 79, wherein the registration authority provides updated license data to the licensing medium when the identifier sent with the registration information corresponds to one of the authorized identifiers.

81. A method according to claim 67, wherein the licensing medium comprises a smart card having a microprocessor and memory.

82. A method according to claim 81, wherein the smart card performs the steps of:

decrypting a first message digest received from the registration authority using a public key associated with the registration authority;

generating a second message digest by performing a hash on updated license data received from the registration authority; and

comparing the first message digest to the second message digest.

83. A method according to claim 67, wherein the license data comprises a licensing medium expiration date determined by a configurable time period during which the licensing medium is valid.

84. A method according to claim 67, wherein the license data comprises a software license expiration date determined by a configurable time period during which access to the electronic data is allowed.

85. A method according to claims 83 or 84, wherein the licensing medium expiration period is set to a shortest software license expiration period of the license data.

86. A method according to claim 67, wherein the license data comprises a software security expiration date determined by a configurable time period during which access to the electronic data is allowed.

87. A method for preventing unauthorized access to electronic data stored on an electronic device, the method comprising the steps of:

storing license data on a portable licensing medium configured to communicate with the electronic device;

determining whether to allow access to the electronic data based on the license data;

verifying, using a registration authority having a first verification database, the license data stored in a second verification database;

verifying the license data stored on the licensing medium using a license manager having the second verification database and being configured to communicate with the electronic device and the registration authority;

providing, using the registration authority, updated verification data for the second verification database of the license manager; and

providing license data to the licensing medium using the license manager.

88. A method according to claim 87, wherein the electronic device verifies validity of the licensing medium by comparing the license data to the second verification database.

89. A method according to claim 87, wherein the license manager verifies the validity of the second verification database by comparing it to the first verification database.

90. A method according to claim 87, wherein the licensing medium stores a license data message digest produced by performing a hash of the license data.

91. A method according to claim 90, wherein the second verification database comprises a copy of the license data message digest.

92. A method according to claim 91, wherein the electronic device verifies validity of the licensing medium by comparing the license data message digest to the copy of the license data message digest in the second verification database.

93. A method according to claim 90, wherein the license data message digest is encrypted with a private key associated with the registration authority or the license manager.

94. A method according to claim 93, wherein the private key is one of a plurality of private keys associated with the registration authority or the license manager.

95. A method according to claim 93, wherein the second verification database comprises a copy of the encrypted license data message digest.

96. A method according to claim 95, wherein the electronic device verifies validity of the licensing medium by comparing the encrypted license data message digest to the copy of the encrypted license data message digest in the second verification database.

97. A method according to claim 95, wherein the electronic device verifies validity of the licensing medium by:

decrypting the license data message digest read from the licensing medium using a public key associated with the registration authority;

generating a message digest by performing a hash on the license data read from the licensing medium; and

comparing the decrypted message digest to the generated message digest.

98. A method according to claim 87, wherein the license manager sends site license registration information to the registration authority.

99. A method according to claim 98, wherein the site license registration information comprises a random identifier associated with the electronic data.

100. A method according to claim 99, wherein the first verification database comprises a list of authorized identifiers that allow access to the electronic data.

101. A method according to claim 100, wherein the registration authority provides updated verification data to the license manager when the identifier sent with the registration information corresponds to one of the authorized identifiers.

102. A method according to claim 87, wherein the license manager communicates with the registration authority to verify that the second verification database corresponds to the first verification database.

103. A method according to claim 87, wherein the license data comprises a licensing medium expiration date determined by a configurable time period during which the licensing medium is valid.

104. A method according to claim 87, wherein the license data comprises a software license expiration date determined by a configurable time period during which access to the electronic data is allowed.

105. A method according to claims 103 and 104, wherein the licensing medium expiration period is set to a shortest software license expiration period of the license data.

106. A method according to claim 87, wherein the license data comprises a software security expiration date determined by a configurable time period during which access to the electronic data is allowed.

107. Computer code executable on an electronic device to prevent unauthorized access to electronic data stored on the electronic device, the computer code comprising:

code for storing license data on a portable licensing medium configured to communicate with the electronic device;

code for determining whether to allow access to the electronic data based on the license data;

code for verifying the license data stored on the licensing medium by communicating with a registration authority having verification data; and

code for providing updated license data received from the registration authority to the licensing medium.

108. A computer program executable on an electronic device to provide access to electronic data stored on the electronic device, the computer program comprising:

code for providing access to the electronic data; and

a subprogram for preventing unauthorized access to the electronic data, the subprogram including:

code for storing license data on a portable licensing medium configured to communicate with the electronic device,

code for determining whether to allow access to the electronic data based on the license data,

code for verifying the license data stored on the licensing medium by communicating with a registration authority having verification data, and

code for providing updated license data received from the registration authority to the licensing medium.

109. Computer code executable on an electronic device to prevent unauthorized access to electronic data stored on the electronic device, the computer code comprising:

code for storing license data on a portable licensing medium configured to communicate with the electronic device;

code for determining whether to allow access to the electronic data based on the license data;

code for verifying, by communicating with a registration authority having a first verification database, the license data stored in a second verification database;

code for verifying the license data stored on the licensing medium by communicating with a license manager having the second verification database and being configured to communicate with the electronic device and the registration authority;

code for providing updated verification data received from the registration authority to the second verification database of the license manager; and

code for providing license data received from the license manager to the licensing medium.

110. A computer program executable on an electronic device to provide access to electronic data stored on the electronic device, the computer program comprising:

code for providing access to the electronic data; and

a subprogram for preventing unauthorized access to the electronic data, the subprogram including:

code for storing license data on a portable licensing medium configured to communicate with the electronic device,

code for determining whether to allow access to the electronic data based on the license data,

code for verifying, by communicating with a registration authority having a first verification database, the license data stored in a second verification database,

code for verifying the license data stored on the licensing medium by communicating with a license manager having the second verification database and being configured to communicate with the electronic device and the registration authority,

code for providing updated verification data received from the registration authority to the second verification database of the license manager, and

code for providing license data received from the license manager to the licensing medium.

111. A method for using a smart card to gain access to protected electronic data on an electronic device, the method comprising the steps of:

transmitting license data stored on the smart card to the electronic device; and

using the electronic device to determine, based on the license data, whether access to the electronic data will be allowed,

wherein the smart card is configured to store updated license data received from the electronic device or from a remote device.

112. A method for using a smart card to gain access to protected electronic data on an electronic device, the method comprising the steps of:

transmitting license data stored on the smart card to the electronic device;

using the electronic device to determine, based on the license data, whether access to the electronic data will be allowed;

communicating, if access to the electronic data is not allowed, with a registration authority having verification data to verify and/or update the license data stored on the smart card; and

storing on the smart card updated license data received from the registration authority.

113. A method for using a smart card to gain access to protected electronic data on an electronic device, the method comprising the steps of:

transmitting license data stored on the smart card to a registration authority having verification data to verify the license data; and

receiving from the registration authority a determination of whether access to the electronic data will be allowed,

wherein the smart card is configured to store updated license data received from the registration authority.

* * * * *

AO 440 (Rev. 12/09) Kallelse i ett civilmål

USA:S DISTRIKTSDOMSTOL

för

Texas östra distrikt

Uniloc USA, Inc. och Uniloc Luxembourg S.A.	)	
_____	)	
Målsägande	)	
mot	)	Civilmål Nr. 6:12-cv-470
Mojang AB	)	
_____	)	
Svarande	)	

KALLELSE I ETT CIVILMÅL

Till: (Svarandens namn och adress) Mojang AB

En stämningsansökan har lämnats in mot dig.

Inom 21 dagar efter delgivningen av denna stämning mot dig (ej inräknat mottagningsdagen) - eller 60 dagar om du är USA eller en myndighet i USA, eller en ämbetsman eller anställd av USA såsom beskrivs i Fed. R. Civ. P. 12 (a)(2) eller (3) — måste du delge målsäganden ett svar till bifogad stämningsansökan eller ett yrkande enligt regel 12 i de federala reglerna för civilmål. Svaret eller yrkandet måste delges målsäganden eller målsägandens advokat, vars namn och adress är:

Barry J. Bumgardner
NELSON BUMGARDNER CASTO, P.C.,
3131 West 7th Street, Suite 300
Fort Worth, Texas 76107
Tel: (817) 377-9111

Om du underlåter att svara kommer tredskodom fällas mot dig för den ersättning som begärs i stämningsansökan. Du måste också registrera ditt svar eller ditt yrkande hos domstolen.

Datum: 7/23/12

UNITED STATES DISTRICT COURT * EASTERN DISTRICT OF TEXAS *

DOMSTOLSNOTARIE

David Maland

Notariens eller biträdande notaries signatur

[Stamp: USA:s distriktsdomstol- Texas östra distrikt]

I USA:s DISTRIKTSDOMSTOL
FÖR TEXAS ÖSTRA DISTRIKT
TYLER-DIVISIONEN

UNILOC USA, INC. och UNILOC LUXEMBOURG S.A.,	§	
målsägande,	§	CIVILMÅL NR. 6:12-cv-470
	§	**RÄTTEGÅNG MED JURY BEGÄRD**
mot	§	
MOJANG AB,	§	
svarande	§	

MÅLSÄGANDENS URSPRUNGLIGA BESVÄRSINLAGA GÄLLANDE PATENTBROTT

Målsäganden Uniloc USA, Inc. ("Uniloc USA") och Uniloc Luxembourg S.A. ("Uniloc Luxembourg") (kollektivt "Uniloc") lämnar in denna ursprungliga besvärsinlaga mot Mojang AB för brott mot patent nr. 6,857,067 ("067 patentet").

PARTERNA

1. Uniloc USA, Inc. ("Uniloc USA") är ett Texas-företag med sitt huvudkontor och huvudsakliga verksamhetsplats i Legacy Town Center I, Suite 380, 7160 Dallas Parkway, Piano. Texas 75024. Uniloc USA har också en verksamhetsplats på 315 North Broadway, Suite 307, Tyler, Texas 75702.

2. Uniloc Luxembourg S.A. ("Uniloc Luxembourg")är ett företag som är organiserat och lyder under Luxemburgs laggar och har sin huvudsakliga verksamhetsplats på 15, rue Edward Steichen. L-2540, Luxemburg.

3. Uniloc Luxembourg och Uniloc USA anges gemensamt som "Uniloc." Uniloc forskar, utvecklar, tillverkar och licensierar teknologiska lösningar för informationssäkerhet,

plattformar och ramverk, inklusive lösningar för att säkra programvaruapplikationer och digitalt innehåll. Unilocs patenterade teknologier möjliggör för programvaru- och innehållsutgivare att på ett säkert sätt distribuera och sälja sin värdefulla teknologitillgångar med minsta möjliga börda för deras legitima slutanvändare. Unilocs teknologi används på flera marknader, inklusive programvaru- och spelsäkerhet, identitetshantering, immaterialrättshantering och viktig infrastruktursäkerhet.

4. Mojang AB ("Mojang") är organiserad och lyder under svensk lag med sin huvudsakliga verksamhetsplats i Stockholm, Sweden. Enligt information och tro har Mojang verksamhet i staten Texas och i Texas östra distrikt.

JURISDIKTION OCH PLATS

5. Uniloc framlägger denna process gällande patentbrott enligt patentlagarna i USA, nämligen 35 U.S.C. §§ 271, 281 och 284-285, bland andra. Denna domstol har jurisdiktion i ämnet i enlighet med 28 U.S.C. §§ 1331, 1338(a) och 1367.

6. Platsen i detta distrikt är lämplig i enlighet med 28 U.S.C. §§ 1391(c) och 1400(b). Enligt information och tro anses svaranden vistas i detta juridiska distrikt, har utfört brottsliga handlingar i detta distrikt, har medvetet genomfört affärer med de anklagade produkterna i detta distrikt och/eller har haft fasta och etablerade verksamhetsplatser i detta juridiska distrikt.

7. Svaranden gäller under denna domstols personliga och allmänna jurisdiktion i enlighet med rättsäkerheten och/eller lagens långa arm i Texas p.g.a. dess avsevärda verksamhet i denna stat och detta juridiska distrikt, inklusive: (A) åtminstone en del av de brottsliga handlingar som hävdas häri; och (B) regelbundet genomförande eller påkallande av

affärer, aktivt utövande av annat ihållande beteende och/eller erhållande av avsevärd avkastning från sålda varor och tillhandahållna tjänster till invånare i Texas.

ÅTALSPUNKT I
(BROTT MOT USA-PATENT NR. 6,857,067)

8. Uniloc införlivar paragraferna 1 till 7 häri genom referens.

9. Uniloc Luxembourg är ägare till, genom tilldelning, av '067-patentet, med titeln "SYSTEM OCH METOD FÖR ATT FÖRHINDRA OBEHÖRIG ÅTKOMST TILL ELEKTRONISKA DATA." En sann och korrekt kopia av '067-patentet är bifogat som Bevis A.

10. Uniloc USA är ensam licenstagare av '067-patentet med ägarskap över alla betydande rättigheter i '067-patentet, inklusive rätten att bevilja underlicenser, utesluta andra och att genomdriva, stämma och ta emot skadestånd för tidigare och framtida brott.

11. '067-patentet är giltigt, verkställbart och vederbörligen utställt i enlighet med Titel 35 USA:s lagsamling.

12. Mojang bryter direkt mot en eller flera punkter i '067-patentet i detta juridiska distrikt och på annan plats i Texas, inklusive åtminstone punkt 107, utan medgivande och tillstånd från Uniloc, med eller genom att tillverka, använda, erbjuda till försäljning, sälja och/eller importera Android-baserade applikationer för användning på mobiltelefoner och/eller surfplattor som kräver kommunikation med en server för att utföra en licenskontroll för att förhindra obehörig användning av sagda applikation, inklusive, men inte begränsat till, Mindcraft.

13. Uniloc har lidit skada som ett resultat av svarandens brottsliga uppförande såsom beskrivs i denna besvärsinlaga. Svaranden är således skyldiga Uniloc ett belopp som på

tillräckligt sätt kompenserar svarandens brott som, enligt lag, inte kan vara mindre än en rimlig royalty, tillsammans med ränta och kostnader såsom fastställs av denna domstol enligt 35 U.S.C. § 284.

BEGÄRAN OM JURY

Uniloc begär härmed rättegång med jury i enlighet med regel 38 i federala regler för civilmål.

BEGÄRAN OM ERSÄTTNING

Uniloc begär att domstolen ser till deras fördel och mot svaranden och att domstolen tilldömer Uniloc följande ersättning:

a. Dom om brott mot en eller flera punkter av '067-patentet, antingen bokstavligt och/eller enligt doktrinen om motsvarande, av svaranden;

b. Dom om att svaranden ska hållas ansvariga för och betala Uniloc för all skada och alla kostnader som Uniloc ådragit sig p.g.a. svarandens brottsliga aktiviteter och annat uppförande som påtalas häri;

c. Dom om att svaranden hålls ansvariga för och betalar Uniloc en rimlig, kontinuerlig, efterdomsroyalty p.g.a. svarandens brottsliga aktiviteter och annat uppförande som påtalas häri;

d. Att Uniloc tilldöms ränta för tiden före och efter domen för de skador som orsakats av svarandens brottsliga aktiviteter och annat uppförande som påtalas häri; och

e. Att Uniloc tilldöms sådan annan ersättning som domstolen anser vara rätt och rimlig under omständigheterna.

Daterat: 20 juli, 2012

Respektfullt inlämnat av,

/s/ Barry J. Bumgardner (med tillåtelse Wesley Hill)
Barry J. Bumgardner
Huvudadvokat
Texas advokatsamfund nr. 00793424
Steven W. Hartsell
Texas advokatsamfund nr. 24040199
NELSON BUMGARDNER CASTO, P.C.
3131 West 7th Street, Suite 300
Fort Worth, Texas 76107

Tel: (817)377-9111
Fax: (817) 377-3485

James L. Etheridge
Texas advokatsamfund nr. . 24059147
ETHERIDGE LAW GROUP, PLLC
2600 E. Southlake Blvd., Suite 120 / 324
South lake, Texas 76092
Telefon: (817) 470-7249
Fax: (817) 887-5950
Jim@EtheridgeLaw.com

T. John Ward, Jr.
Texas advokatsamfund nr. 00794818
E-mail: jw@wsfirm.com
J. Wesley Hill
Texas advokatsamfund nr. . 24032294
E-POST: WH@VVSFIRM.COM
WARD & SMITH LAW FIRM
P.O. Box 1231
1127 Judson Rd., Ste. 220
Longview, Texas 75606-1231
(903)757-6400
(903) 757-2323 (fax)

Målsägandens advokater
Uniloc USA, Inc. och Uniloc Luxembourg S.A.

JS44 (Rev.09/11)

CIVILMÅL FÖRSÄTTSBLAD

Försättsbladet JS 44 och den information som anges häri varken ersätter eller kompletterar registreringen och delgivningen av pläderingar eller andra papper som lagen kräver, förutom så som föreskrivet av lokala domstolsregler. Detta formulär, godkänd av USA:s domstolskonferens i september 1974, krävs för användning av domstolsnotarie i syfte att påbörja det civila dokumentationsbladet. ***(SE INSTRUKTIONER PÅ NÄSTA SIDA AV DETTA FORMULÄR.)***

I. (a) MÅLSÄGANDEN
UNILOC USA. INC. och UNILOC LUXEMBOURG S.A.

(b) Bosättningsland för först listade målsägande_____
(UTOM I MÅLSÄGANDEFALL I USA)

(c) Advokater *(Firmanamn, adress och telefonnummer)*
Barry J. Bumgardner, NELSON BUMGARDNER CASTO. P.C., 3131 West 7th Street, Suite 300, Fort Worth, Texas 76107, Tel: (817) 377-9111

SVARANDEN
MOJANG AB

Bosättningsland för först listade svarande_____
(ENDAST I MÅLSÄGANDEFALL I USA)

OBS: I LANDKONFISKERINGSFALL, ANVÄND PLATSEN FÖR DEN LANDEGENDOM FALLET GÄLLER.

Advokater *(om känt)*

II. GRUND FÖR JURISDIKTION *(Markera endast en ruta)*

☐ 1 USA:s regering målsägande
☒ 3 Federal fråga *(USA:s regering ej part)*
☐ 2 USA:s regering svarande
☐ 4 Mångfald *(Ange parternas medborgarskap i del III)*

III. HUVUDPARTERNAS MEDBORGARSKAP *(Endast i mångfaldsmål)* *(Sätt ett kryss i en ruta för målsäganden och i en ruta för svaranden)*

	MÅL	SVA		MÅL	SVA
Medborgare i denna stat	☐ 1	☐ 1	Införlivad *eller* huvudsaklig verksamhetsplats i denna stat	☐ 4	☐ 4
Medborgare i annan stat	☐ 2	☐ 2	Införlivad *och* huvudsaklig verksamhetsplats i annan stat	☐ 5	☐ 5
Medborgare eller invånare i annat land	☐ 3	☐ 3	Annat land	☐ 6	☐ 6

IV. PROCESSENS NATUR *(Markera endast en ruta med ett "X")*

KONTRAKT	ÅTALBRA HANDLINGAR		FÖRVERKANDE/VITE	KONKURS	ÖVRIGA STADGAR
☐110 Försäkring	PERSONSKADOR	PERSONSKADOR	☐625 Drogrelaterad konfiskering av egendom **21 USC 881**	☐422 Överklagan 28 USC 158	☐375 Lagen om falska anspråk
☐120 Marint	☐310 Flygplan	☐365 Personskador – Produktansvar	☐690 övrigt	☐423Tillbakadragning 28 USC 157	☐400 Statsomfördelning
☐130 Millerlagen	☐315 Flygplan produktansvar	☐367 Hälsovårds-/ farmaceutiska personskador produktansvar			☐410 Antitrust
☐140 Förhandlingsbart instrument	☐320 Övergrepp, kränkning & förtal	☐368 Asbest personskador Produktansvar		EGENDOMSRÄTT	☐430 Banker och bankväsende
☐150 Återtagande av överbetalning & genomdrivande av dom	☐330 Federala anställdas ansvar	PRIVAT EGENDOM		☐820 Copyright	☐450 Kommers
☐151 Vårdlagen	☐340 Marint	☐370 Övriga bedrägerier		☒830 Patent	☐460 Deportering
☐152 Återtagande av förfallna studielån (Exkl. veteraner)	☐345 Marint produktansvar	☐371 Ärlighet vid utlåning		☐840 Varumärken	☐470 Utpressning påverkade och korrupta organisationer
☐153 Återtagande av överbetalning av veteranförmåner	☐350 Motorfordon	☐380 Annan privat egendomsskada	ARBETE	SOCIALBIDRAG	☐480 Kundkredit
☐160 Aktieägarprocesser	☐355 Motorfordon Produktansvar	☐385 Egendomsskada produktansvar	☐710 Lagen om rättvisa arbetsförhållanden	☐861 HIA (1395ff)	☐490 Kabul-/Sat. TV
☐190 Övriga kontrakt	☐360 Övriga personskador		☐720 Arbete/ledn. relationer	☐862 Koldammlunga (923)	☐850 Värdepapper/råvaror/ börshandel
☐195 Kontrakt produktansvar	☐362 Personskador – Med. felbehandling		☐740 Järnvägsarbetslagen	☐863 DIWC/DIWW (405(g))	☐890 Andra lagenliga processer
☐196 Franchise			☐751 Lagen om familjerelaterad och medicinsk	☐864 SSID Titel XVI	☐891 Jordbrukslagar
				☐865 RSI (405(g))	☐893 Miljöfrågor
					☐895 Informationsfrihetslagen
					☐896 Förlikning
					☐899 Administrativa processer

REALEGENDOM	CIVILA RÄTTIGHETER	BEGÄRAN, INTERNER	ledighet	FEDERALA SKATTEPROCESSER	Lag/granskning eller överklagan av ett myndighetsbeslut
☐210 Landkonfiskering ☐220 Pantövertagande ☐230Hyreskontrakt & vräkning ☐240Åtalbar handling, land ☐245 Åtalbar handling, produktansvar ☐290 All övrig realegendom	☐440 Övriga civila rättigheter ☐441 Rösträtt ☐442 Anställning ☐443 Inhysning/boende ☐445 Amer. med funktionshinder – anställning ☐446 Amer. med funktionshinder – övrigt ☐448 Utbildning	☐510 Begäran om upphävt straff **Habeas Corpus:** ☐530 Allmänt ☐535 Dödsstraff ☐540 Åläggande & övrigt ☐550 Medborgerliga rättigheter ☐555 Fängelseförhållanden ☐560 Civila fångar– inlåsningsförhållanden	☐790 Övriga arbetsprocesser ☐791 Lagen om anställds inkomsttrygghet **IMMIGRATION** ☐462 Naturaliseringsansökan ☐463 Habeas Corpus – Utländsk intern (begäran, interner) ☐465 Övriga immigrationsprocesser	☐870 Skatter (USA målsägande eller svarande) ☐871 Skatteverket—tredje part 26 USC 7609	☐950 USA:s konstitution

V. URSPRUNG *(Markera endast en ruta med ett "X")*

☒1 Ursprunglig process ☐2 Flyttad från statlig domstol ☐3 Återsänd från appellationsdomstol ☐4 Återupptagen eller återöppnad ☐5 Överförd från annat distrikt *(specificera)* ☐6 Flerdistrikts-process

VI. PROCESSENS ORSAK

Ange den USA-civillag under vilken du stämmer *(Ange inte jurisdiktionslagar om de inte skiljer sig)*:
35 U.S.C.§§271, 281, och 284-285

Kort beskrivning av orsaken:
patentbrott

VII. ÖNSKEMÅL I BESVÄRSINLAGAN:

☐ MARKERA OM DETTA ÄR EN **GRUPPTALAN** UNDER F.R.C.P. 23

BEGÄRAN $

MARKERA JA endast om det begärs i besvärsinlagan:

JURY BEGÄRD ☒ Ja ☐ Nej

VIII. RELATERADE FALL OM NÅGRA *(Se introduktioner):*

DOMARE **SE BILAGA**

DOCKETNUMMER **SE BILAGA**

DATUM
20/7, 2012

REGISTRERAD ADVOKATS UNDERSKRIFT
/s/ Barry J. Bumgardner (m/tillstånd Wesley Hill)

ENDAST FÖR KONTORSANVÄNDNING

MOTTAGET_____ BELOPP _____ SÖKANDE IFP _____ DOMARE _____ SKILJ. DOM_____

RELATERADE FALL

DOKUMENTATIONSNUMMER:

6:12-cv-462 - DOMARE EJ UTSEDD
6:12-cv-463 - DOMARE EJ UTSEDD
6:12-cv-464 - DOMARE EJ UTSEDD
6:12-cv-466 - DOMARE EJ UTSEDD
6:12-cv-467 - DOMARE EJ UTSEDD
6:12-cv-468 - DOMARE EJ UTSEDD
6:12-cv-469 - DOMARE EJ UTSEDD

Bevis "A"

US006I857067B2

(12) **USA-patent**
Edelman

(10) **Patent nr.: US 6,857,067 B2**
(45) **Patentdatum: 15 feb. 2005**

(54) **SYSTEM OCH METOD FÖR FÖRHINDRANDE AV OBEHÖRIG ÅTKOMST TILL ELEKTRONISKA DATA**

(76) Uppfinnare: **Martin S. Edelman,** 11 Lake Ontario La., Morganville, NJ (US) 07751

(*) Notering: Gällande någon ansvarsfriskrivning, villkoren för detta patent är förlängda eller justerade enligt 35 U.S.C. 154(b) med 641 dagar.

(21) Ansök. nr.: **09/792,045**

(22) Reg.: **Feb. 26, 2001**

(65) **Tidigare publiceringsdata**

US 2002/0029347 A1 7 mars, 2002

Relaterade USA-ansökningsdata

(60) Preliminärt ansökningsnr. 60/229,934, reg. 1 sept, 2000.

(51) **Int. Cl.**[7] **G06F**

6,009,401 A	12/1999	Horstmann	705/1
6,009,525 A	12/1999	Horstmann	713/200
6,021,438 A	2/2000	Duvvoori et al	709/224
6,023,766 A	2/2000	Yamamura	713/201
6,029,145 A	2/2000	Barritz et al	705/34
6,047,242 A	3/2000	Vaeth et al	713/201
6,035,402 A	4/2000	Benson	702/35
6,049,789 A	4/2000	Frison et al	705/59
6,067,582 A	5/2000	Smith et al	710/5
6,073,123 A	6/2000	Staley	705/58
6,078,909 A	6/2000	Knutson	705/59
6,087,955 A	7/2000	Gray	340/825.34
6,101,606 A	8/2000	Diersch et al	713/201
6,128,741 A	10/2000	Goetz et al	713/200

ÖVRIGA PUBLIKATIONER

Charles Cagliostro, "Rosy Outlook Predicted for US Smartkort Market", Card Forum International, pp. 45-47, Nov./ Dec. 1999.
Carol H. Fancher, "Smartkorts", Scientific American, pp. 1-10,

1/26
(52) **U.S. Cl.** **713/1.55;** 713/182; 713/200; 713/201
(58) **Sökfält** 713/155, 182, **713**/200, 201

(56) **Åberopade referenser**

USAPATENTDOKUMENT

5,502,764 A	3/1996	Naccache	380/23
5,826,011 A	10/1998	Chou et al.	395/186
5,844,497 A	12/1998	Gray	340/825.34
5,933,498 A	8/1999	Schneck et al.	380/4
5,935,246 A	8/1999	Benson	713/200
5,940,504 A	8/1999	Griswold	380/4
5,956,404 A	9/1999	Schneier et al.	380/25
5,987,134 A	11/1999	Shin et al.	380/25
6,008,737 A	12/1999	Deluca et al.	340/825.34

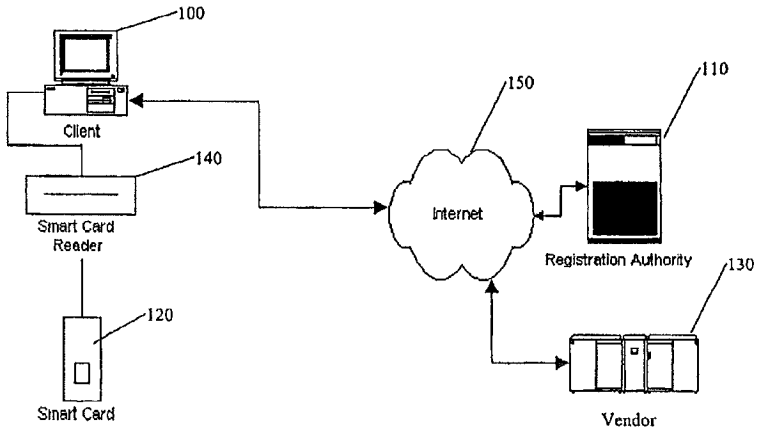
Aug. 1996.

Primary Examiner—Thomas R. Peeso
(74) *Attorney, Agent, or Firm*—Fitzpatrick, Cella, Harper & Scinto

(57) **ABSTRAKT**

Ett system och en metod tillhandahålls för att förhindra obehörig åtkomst till elektroniska data som lagras på en elektronisk enhet. Ett portabelt licensmedium konfigureras för att kommunicera med den elektroniska enheten för lagring av licensdata. Licensdata avgör om åtkomst ska beviljas till elektroniska data. En registreringsinstans kommunicerar med den elektroniska enheten. Registreringsinstansen har en databas av verifikationsdata för att bekräfta licensdata som lagras på licensmediet och tillhandahåller uppdaterad licensdata till licensmediet.

113 Anspråk, 9 ritningsblad



Client	Klient
Smart Card	Smartkort
Smart Card Reader	Smartkortläsare
Internet	Internet
Registration Authority	Registreringsinstans
Vendor	Säljare

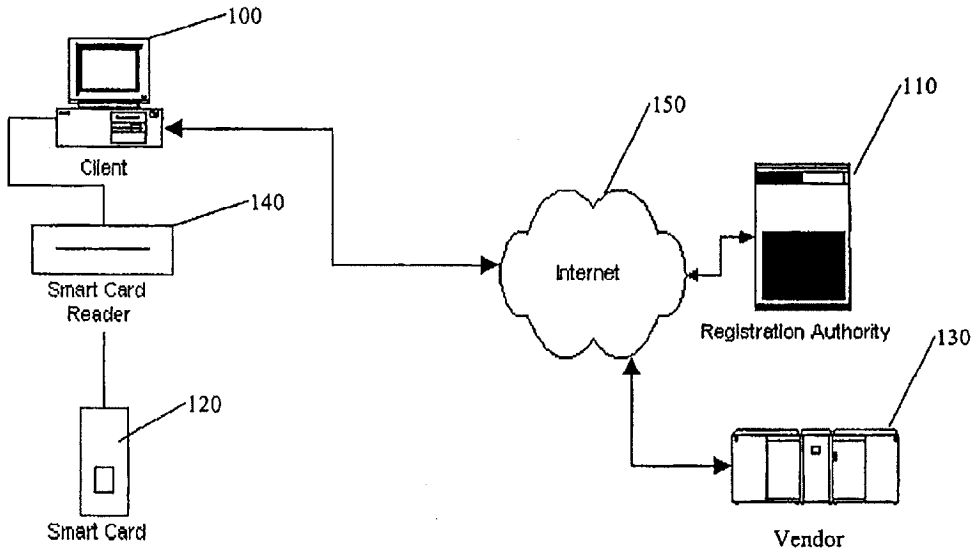


Bild 1

Client	Klient
Smart Card	Smartkort
Smart Card Reader	Smartkortläsare
Internet	Internet
Registration Authority	Registreringsinstans
Vendor	Säljare

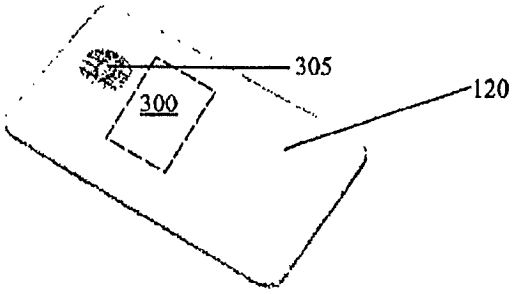


Bild 2

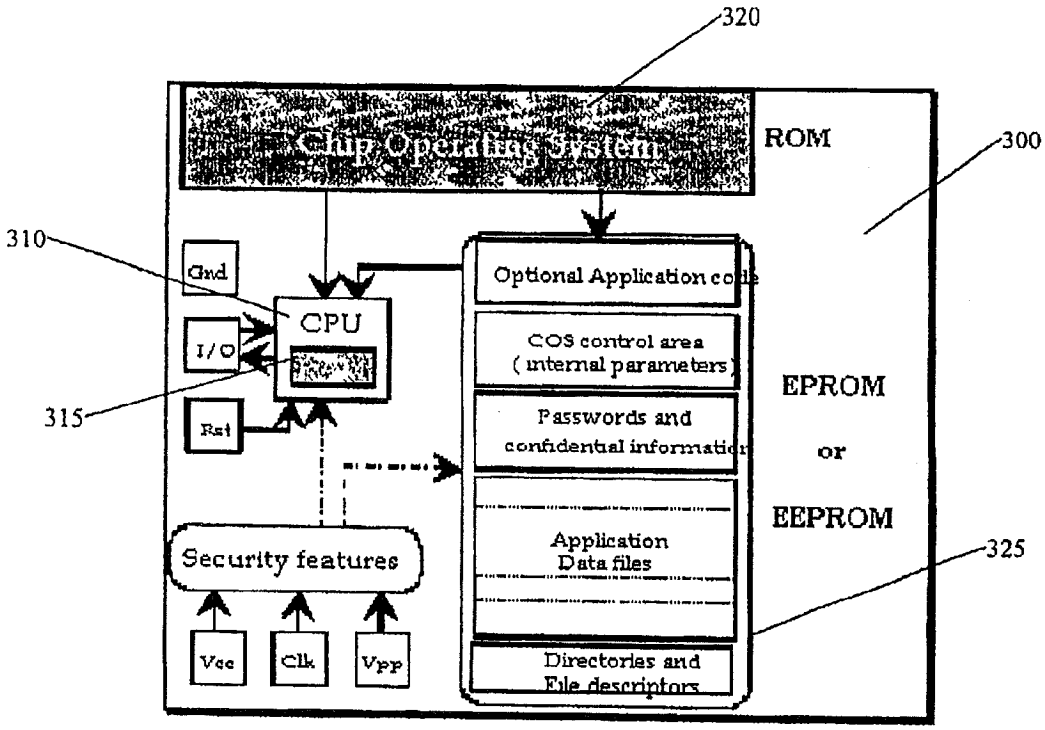


Bild 3

Chip Operating System	**Chip operativsystem**
Optional Application code	**Valfri applikationskod**
Cos control area (internal parameters)	**Cos kontrollområde (interna parametrar)**
Passwords and confidential information	**Lösenord och konfidentiell information**
Application Data files	**Applikationsdatafiler**
Directories and File descriptors	**Register och fildeskriptorer**
ROM	**ROM**
EPROM or EEPROM	**EPROM eller EEPROM**
Gnd	**Gnd**
Rst	**Rst**
CPU	**CPU**
Security features	**Säkerhetsfunktioner**
Vcc	**Vcc**
Clk	**Clk**
Vpp	**Vpp**

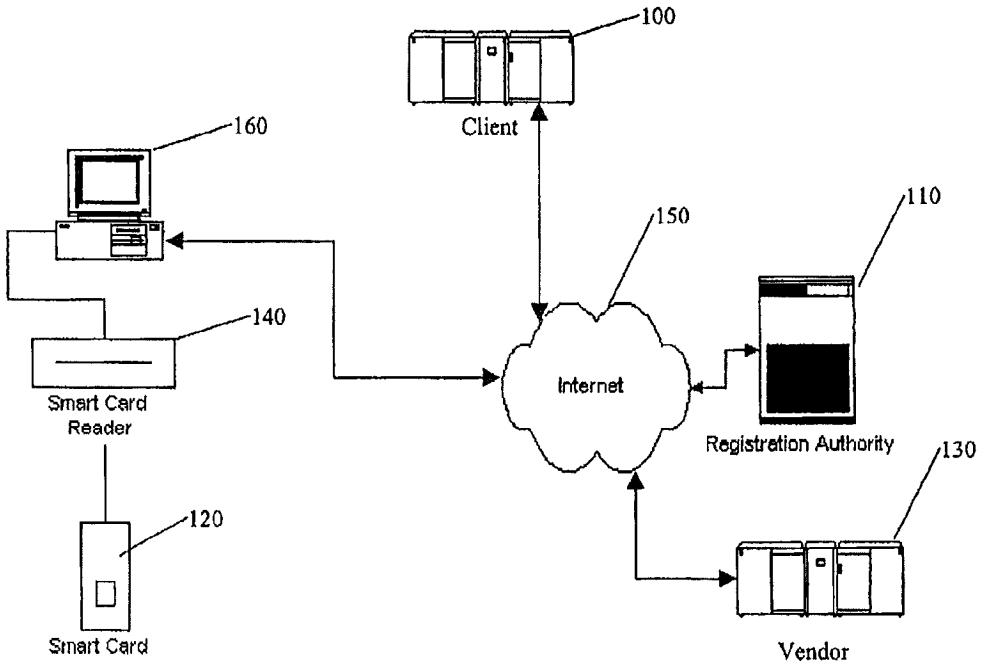


Bild 4

Client	Klient
Smart Card	Smartkort
Smart Card Reader	Smartkortläsare
Internet	Internet
Registration Authority	Registreringsinstans
Vendor	Säljare

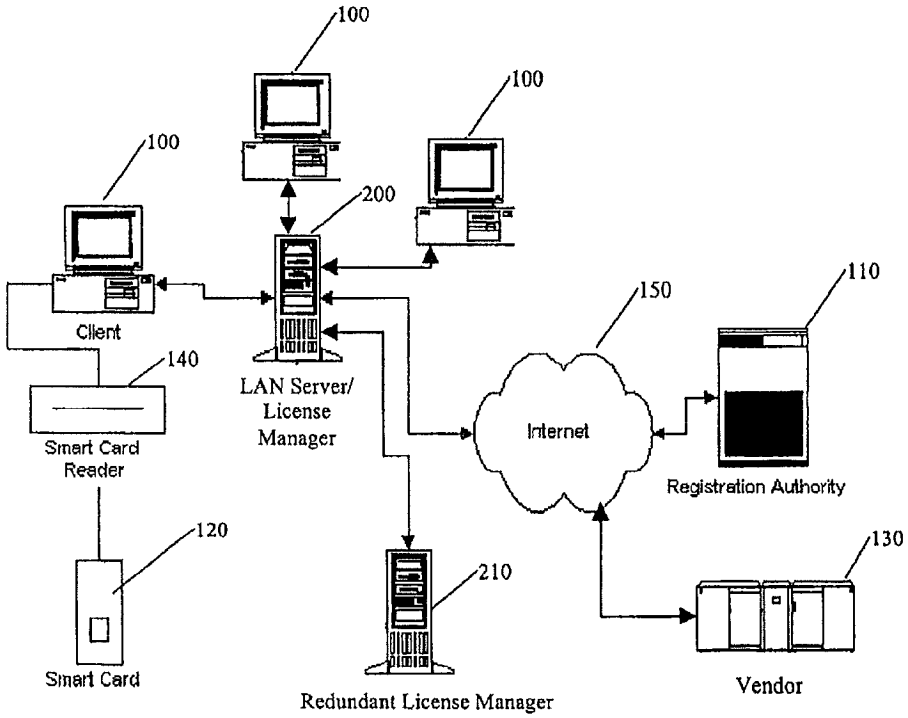


Bild 5

Smart Card	Smartkort
Smart Card Reader	Smartkortläsare
LAN Server/License Manager	LAN-server/Licenshanterare
Redunant License Manager	Övertalig licenshanterare
Internet	Internet
Registration Authority	Registreringsinstans
Vendor	Försäljare

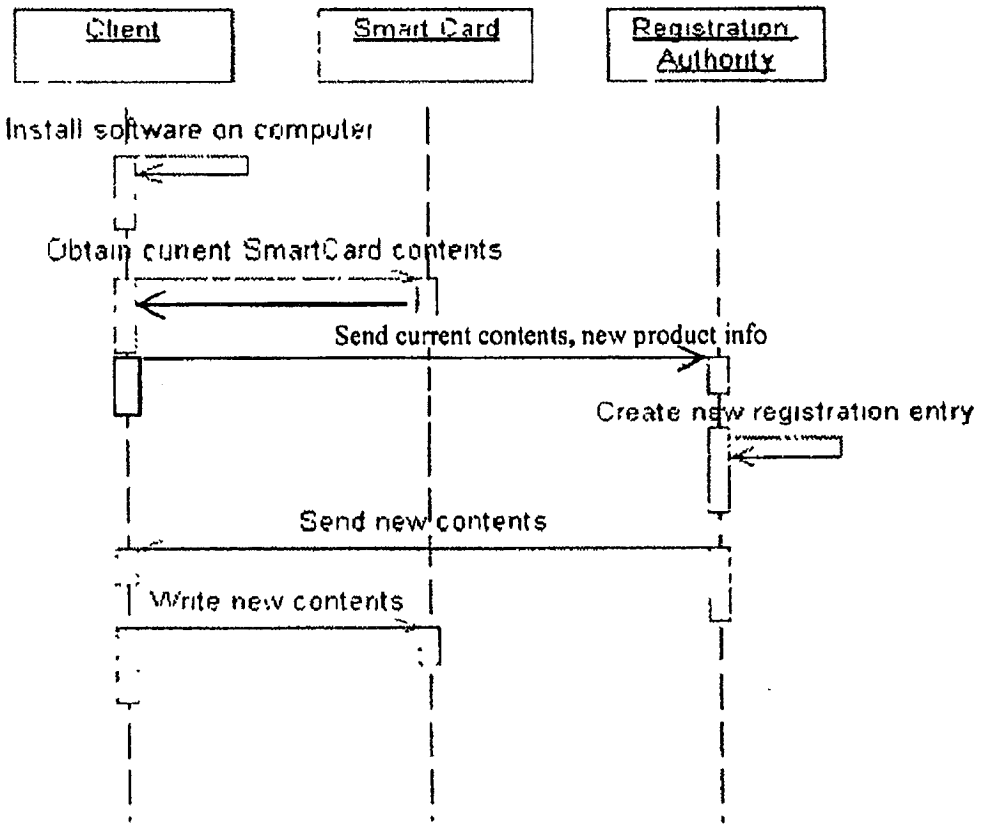


Bild 6

Client	Klient
Smart Card	Smartkort
Registration Authority	Registreringsinstans
Install software on computer	Installera mjukvara på dator
Obtain current SmartCard contents	Hämta aktuellt SmartCard-innehåll
Send current contents, new product info	Skicka aktuellt innehåll, ny produktinfo
Create new registration entry	Skapa nytt registreringsinlägg
Send new contents	Skicka nytt innehåll
Write new contents	Skriv nytt innehåll

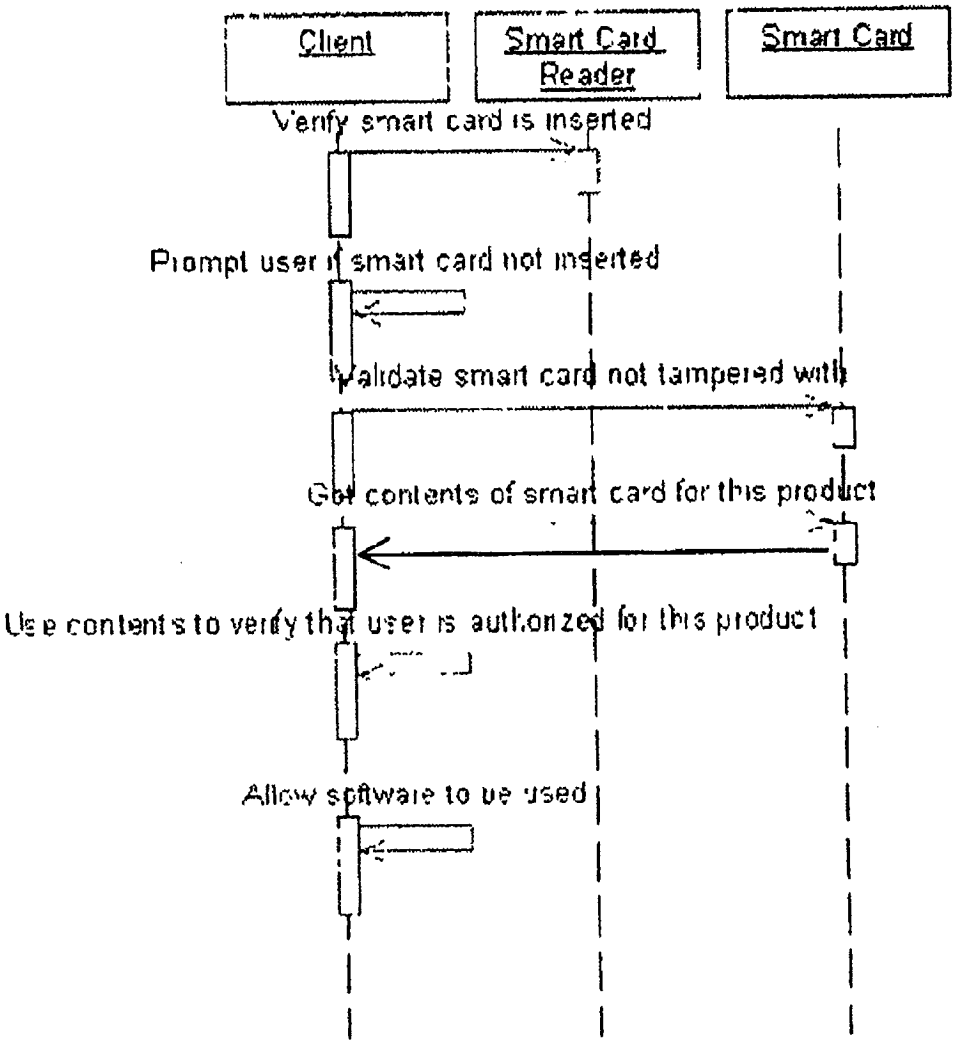


Bild 7

Client	Klient
Smart Card Reader	Smartkortläsare
Smart Card	Smartkort
Verify smart card is inserted	Säkerställ att smartkort är isatt

Prompt user if smart card not inserted	Uppmana användare om smartkort inte är isatt
Validate smart card not tampered with	Säkerställ att smartkort är omanipulerat
Get contents of smart card for this product	Hämta smartkortinnehåll för denna produkt
Use contents to verify that user is authorized for this product	Använd innehåll för att bekräfta att användaren är behörig för denna produkt
Allow software to be used	Tillåt att mjukvaran används

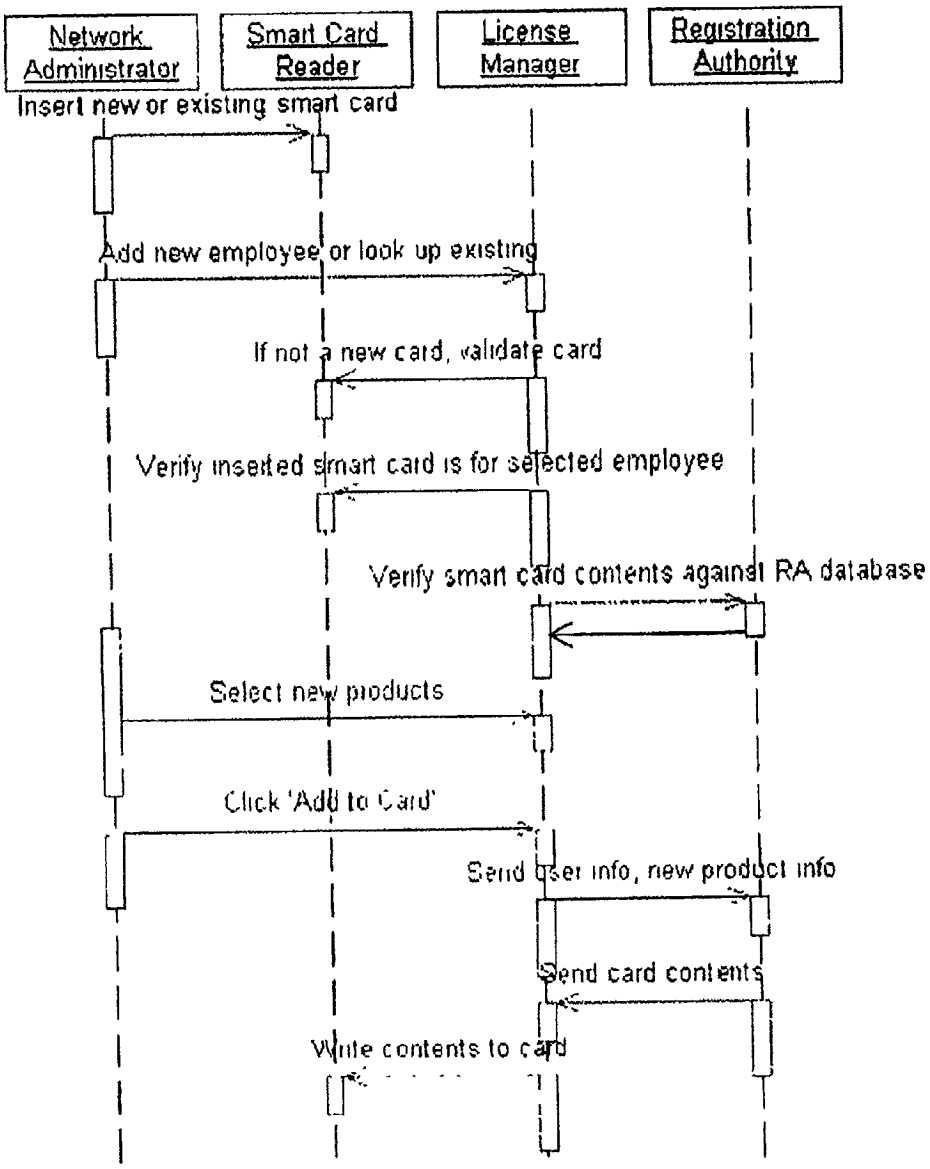


Bild 8

Network Administrator	Nätverksadministratör
Smart Card Reader	Smartkortläsare
License Manager	Licenshanterare
Registration Authority	Registreringsinstans
Insert new or existing smart card	Sätt i nytt eller befintligt smartkort
Add new employee or look up existing	Lägg till ny anställd eller leta upp befintlig
If not a new card, validate card	Om det inte är ett nytt kort, verifiera kort
Verify inserted smart card or selected employee	Verifiera isatt smartkort eller vald anställd
Verify smart card contents against RA database	Verifiera smartkortsinnehåll mot REn-databasen
Select new products	Välj nya produkter
Click "Add to card"	Klicka på "Lägg till på kort"
Send user info, new product info	Skicka användarinfo, ny produktinfo
Send card contents	Skicka kortinnehåll
Write contents to card	Skriv innehåll till kort

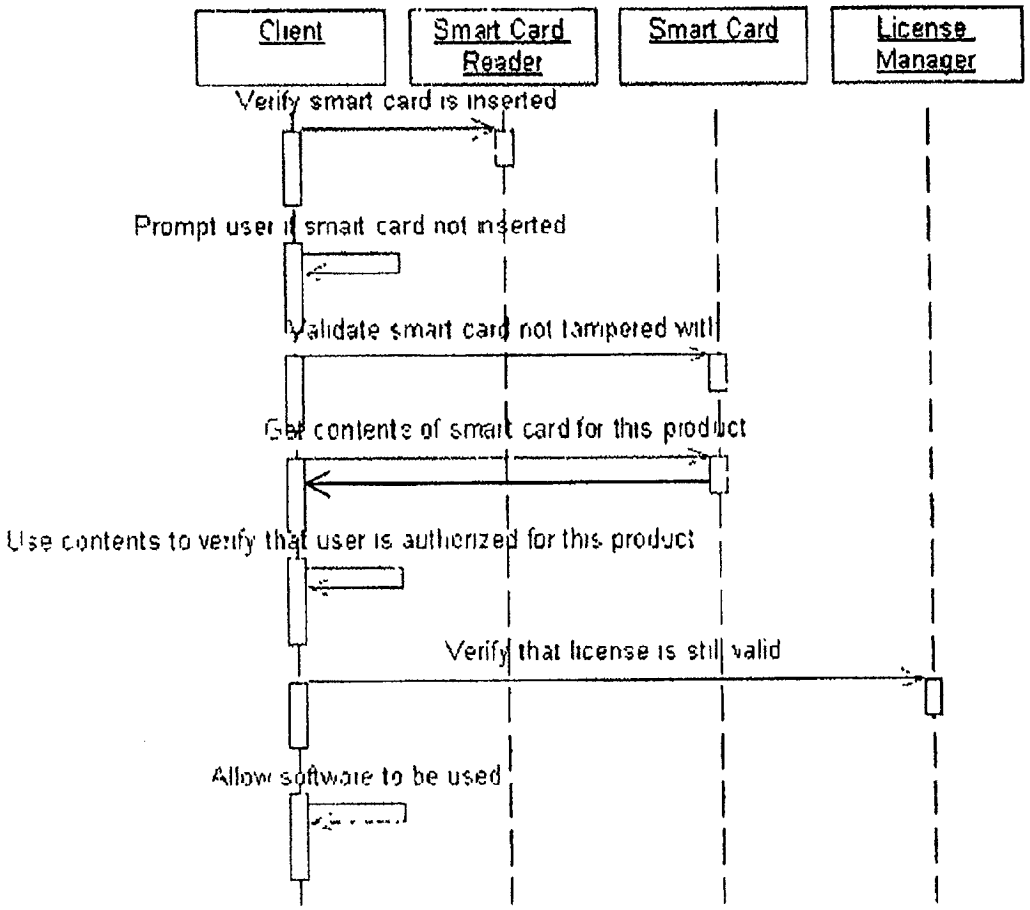


Bild 9

Client	Klient
Smart Card	Smartkort
Smart Card Reader	Smartkortläsare
License Manager	Licenshanterare
Verify smart card is inserted	Säkerställ att smartkort är isatt
Prompt user if smart card not inserted	Uppmana användare om smartkort inte är isatt
Validate smart card not tampered with	Säkerställ att smartkort är omanipulerat
Get contents of smart card for this product	Hämta innehåll på smartkort för denna produkt
Use contents to verify that user is authorized for this product	Använd innehåll för att verifiera att användaren är behörig för denna produkt
Verify that license is still valid	Säkerställ att licensen fortfarande är giltig
Allow software to be used	Tillåt att mjukvaran används

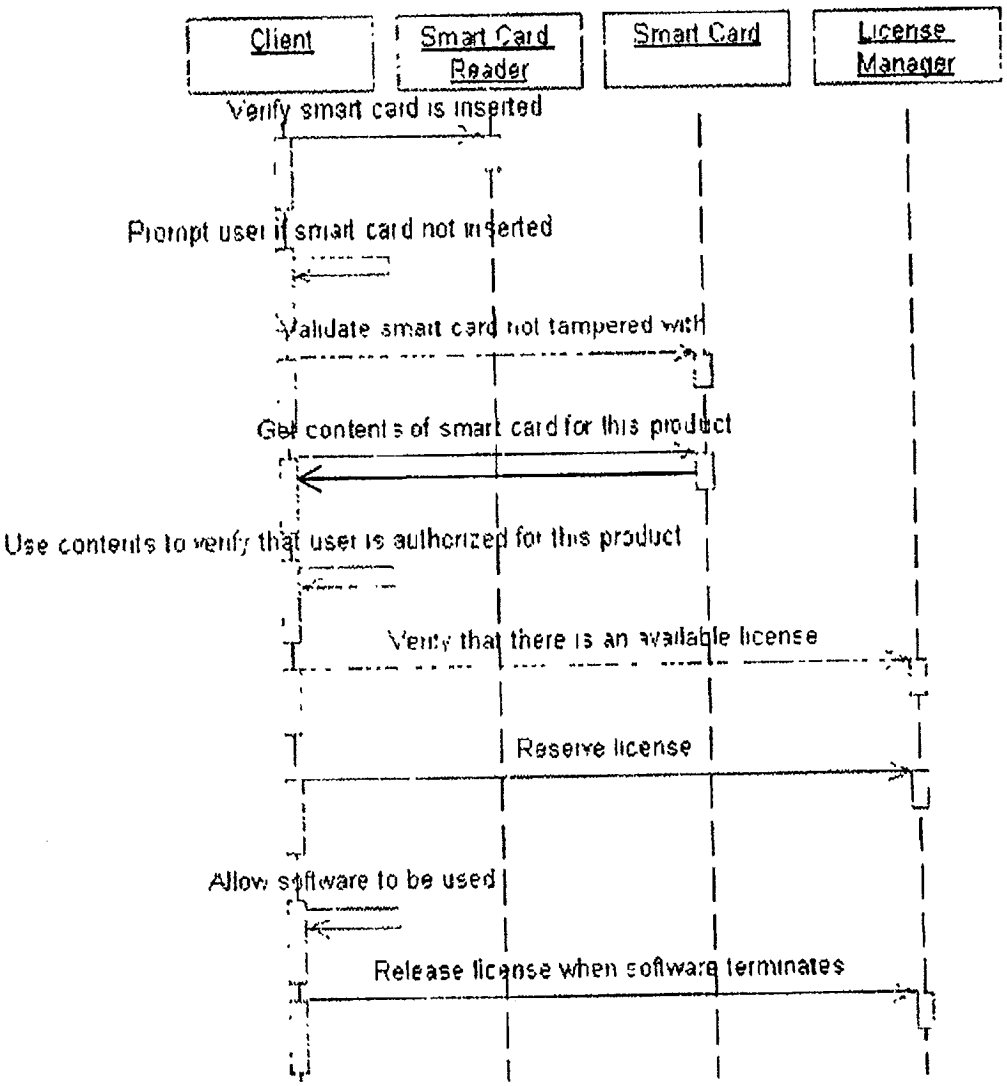


Bild 10

Client	Klient
Smart Card Reader	Smartkortläsare
Smart Card	Smartkort
License Manager	Licenshanterare
Verify smart card is inserted	Säkerställ att smartkort är isatt
Prompt user if smart card not inserted	Uppmana användare om smartkort inte är isatt
Validate smart card not tampered with	Säkerställ att smartkortet är omanipulerat
Get contents of smart card for this product	Hämta innehåll på smartkort för denna produkt
Use contents to verify that user is authorized for this product	Använd innehåll för att säkerställa att användaren är behörig för denna produkt
Verify that there is an available license	Säkerställ att det finns en tillgänglig licens
Reseive license	Ta emot licensen
Allow software to be used	Tillåt att mjukvaran används
Release license when software terminates	Släpp licensen när mjukvaran avslutas

SYSTEM OCH METOD FÖR FÖRHINDRANDE AV OBEHÖRIG ÅTKOMST TILL ELEKTRONISKA DATA

Denna ansökan hävdar fördelarna med USA Preliminär ansökan nr. 60/229,934, reg. 1 sept, 2000.

UPPFINNINGENS BAKGRUND

1. Uppfinningsområde

Den aktuella uppfinningen handlar om att förhindra obehörig åtkomst till elektroniska data, som exempelvis datormjukvara, musik, filmer, e-böcker och liknande. Mer specifikt handlar den aktuella uppfinningen om ett åtkomstbehörighetssystem och en metod med vilken en elektronisk klientenhet kommunicerar med ett licensmedium som lagrar licensdata som identifierar de elektroniska data till vilken användaren är behörig att ha tillgång till. Den elektroniska klientenheten kommunicerar med en central registreringsinstans som innehåller en databas som används för att bekräfta licensdata.

2. Relaterad konst

Elektroniska enheter, både stationära och trådlösa, såsom persondatorer, handhållna datorenheter, personliga dataenheter, mobiltelefoner och CD- och DVD-spelare är allmänt förekommande. Dessa enheter utför ett ökande antal funktioner, inklusive affärer, underhållning och funktioner av undervisande typ, för att bara nämna några.

Den gemensamma nämnaren mellan dessa enheter är deras användning av elektroniska data för att utföra sina respektive funktioner. Dessa elektroniska data kan användas för att kontrollera själva enheten, såsom när data utgör ett mjukvaruprogram för en dator. Alternativt kan elektroniska data vara intellektuellt innehåll som manipuleras av dessa enheter, såsom exempelvis när data utgör musik, filmer, e-böcker, databasinformation eller andra typer av data som är privilegierade, copyrightskyddade, äganderättsskyddade eller på annat sätt skyddade för obehörig åtkomst

Oavsett vilket så är elektronisk data värdefull på grund av den tid och energi som lagts ner vid skapandet av data. Exempelvis så är ett mjukvaruprogram för en dator produkten av en mycket arbetsintensiv utveckling som involverar mjukvaruingenjörer, programmerare, konstnärer och marknadsförare, för att bara nämna några. På samma sätt är musik, filmer och e-böcker produkter av kreativa ansträngningar från artister, konstnärer och författare. Dessutom kan skapandet av alla dessa elektroniska data innebära mycket höga produktionskostnader och marknadsföringsansträngningar.

I kontrast till detta krävs det vanligtvis väldigt lite tid, ansträngning och pengar för att kopiera sådana elektroniska data. Som en konsekvens är obehörig kopiering och distribution av elektroniska data mycket omfattande. När det gäller mjukvara för persondatorer, till exempel, beräknas det att 30 % av den mjukvara som används i USA är olicensierad och således obehörig.

I vissa andra länder är mer än 95 % av den mjukvara som används obehöriga kopior som skapas i USA eller på andra platser och säljs till en liten del av det amerikanska detaljhandelspriset. I vissa av dessa länder har piratkopiering av mjukvara blivit till en stor industri. Denna omfattande obehöriga användning av mjukvara och andra elektroniska data har en potentiellt avkylande effekt på artister, entreprenörer och andra som skapar dem.

Lagen tillhandahåller naturligtvis vissa mekanismer för att förhindra och avskräcka mot sådan piratverksamhet. Copyrightskydd är exempelvis ett av de vanligaste lagliga medlen för skydd av elektroniska data. Patentskydd används också i ökad utsträckning för att skydda vissa elektroniska data, speciellt

olika typer av datormjukvara. Kontraktuella villkor, såsom licenser, används ofta som komplement till andra typer av skydd.

Rätten att använda mjukvara kan begränsas till en enskild användare eller en enskild dator. När användande på fler än en dator övervägs, såsom i ett lokalt nätverk (LAN), kan licensen tillåta användning på flera datorer. Den här sortens licens för flera datorer kallas ofta platslicens eftersom den vanligtvis används på flera datorer på en specifik plats som använder den licensierade mjukvaran.

Effektiviteten hos dessa juridiska och kontraktuella åtgärder har dock varit otillräcklig. Således har försäljare av elektroniska data tagit till tekniska åtgärder för att skydda sitt immateriella innehåll.

Exempelvis kan licensierade elektroniska data, såsom datormjukvara, skyddas från obehörig användning och/eller kopiering genom att man använder en skyddsplan som innebär att användaren måste registrera den licensierade mjukvaran hos säljaren. Vanligen använder sådana skyddsplaner ett registreringsprogram som inkluderas i mjukvaran och startas vid installationen av mjukvaran.

Registreringsprogrammet kräver att användaren anger en kodsekvens som tillhandahölls av användaren tillsammans med mjukvaran, t.ex. tryckt på ett CD-fodral. Kodsekvensen kontrolleras av registreringsprogrammet för att avgöra om den är giltig. Om den är giltig tillåter registreringsprogrammet att användaren använder mjukvaran.

Konventionella registreringsprogram fastställer kodsekvensens validitet med hjälp av matematiska algoritmer. Vanligtvis är dessa algoritmer en omkastning av den algoritm som från början användes av säljaren för att generera den uppsättning giltiga kodsekvenser som tillhandahölls med mjukvaran.

Även om sådana konventionella planer ger en grundläggande säkerhet så är de långt från oslagbara. Faktum är att sådana säkerhetssystem ofta omintetgörs av pirater som räknar ut algoritmerna för att fastställa validitet genom att analysera kodsekvenserna som de genererar. När en algoritm har räknats ut kan den användas av obehöriga användare för att skapa giltiga kodsekvenser för den licensierade mjukvaran. Dessa giltiga kodsekvenser eller själva algoritmen, som kallas en keygen, kan sedan distribueras till ett mycket omfattande antal obehöriga användare. Många keygens för många kommersiellt framgångsrika licensierade mjukvaruprodukter finns faktiskt gratis att tillgå på Internet.

Vissa säljare har försökt att förbättra sin plan för kodsekvensskydd genom att kräva att användare anger viss privat information, såsom användarnamn och telefonnummer. Denna information överförs till säljaren där den kodas och används i genereringsprocessen för kodsekvensen. Kodsekvensen skickas tillbaka till användaren som använder den för att låsa upp mjukvaran. Dock är detta tillvägagångssätt, liksom tillvägagångssättet för kodsekvenser som tas upp ovan, också baserade på uträkningsbara matematiska algoritmer och därför går de, av samma anledning, att gå runt.

Ett annat tillvägagångssätt för att förhindra obehörig åtkomst till licensierad mjukvara är att kräva att användaren har hårdvarunycklar, så kallade donglar, anslutna till datorn för att kunna använda den licensierade mjukvaran. Vanligtvis är donglar anslutna till en in-/utgångsport (I/O) på en dator.

Det finns ett antal nackdelar med användandet av donglar. Till exempel så behöver varje licensierad mjukvara en egen dongel, men datorer har oftast ett begränsat antal I/O-portar. Således kanske flera donglar måste kopplas till en enda I/O-port om flera

Licensierade mjukvaror ska användas. Detta kan leda till störningar mellan de olika donglarna, vilket kan leda till att donglarna eller deras respektive mjukvara inte fungerar. En annan nackdel är att donglar lätt kan tappas bort eller stjälas. Mjukvarulicensgivare ersätter vanligtvis förlorade eller stulna donglar till en mindre avgift, vilket kan låta obehöriga användare få enkel tillgång till donglar.

Ett annat tillvägagångssätt för att förhindra obehörig användning och/eller kopiering av licensierad mjukvara är att kräva att användaren har en licensmodul kopplad till användarnätverket för att kunna använda den licensierade mjukvaran. Detta tillvägagångssätt tas upp i USA Pat. Nr. 6,101,606 (Diersch et al.). Modulen kan innehålla en identifieringskod och annan licensinformation. Den licensierade mjukvaran kommunicerar regelbundet med licenshanteringsmjukvaran på en nätverksserver. Licenshanteringsmjukvaran kommunicerar i sin tur med licensmodulen för att fastställa om en giltig modul är ansluten till nätverket.

Det finns flera nackdelar med tillvägagångssättet med en licensmodul. Licensmodulen innehåller en fast identifieringskod som kan utrönas genom analys av modulen. Att utröna identifieringskoden skulle kunna låta obehöriga användare att duplicera modulen. En annan nackdel med tillvägagångssättet med en licensmodul är att den är känslig för manipulation. Exempelvis kanske en användare ökar antalet obehöriga användare för en platslicens genom att ändra den licensdata som finns lagrad i modulen.

Ännu en nackdel med tillvägagångssättet med en licensmodul är att behöriga användare inte kan använda den licensierade mjukvaran på en dator som inte är uppkopplade mot det enskilda fasta nätverket. Exempelvis kan en behörig användare inte använda den licensierade mjukvaran på en bärbar dator, personlig digital enhet eller andra typer av mobila datorenheter.

Ett annat tillvägagångssätt för att förhindra obehörig användning och/eller kopiering av licensiera mjukvara är att tillhandahålla licenshanteringsmjukvara som installeras på användarens server, så som det tas upp i USA Pat. Nr. 6,049,789 (Frison et al.). Hanteringsmjukvaran skickar licensförfrågningar om pay-per-use (betala per användning) för den licensierade mjukvaran till ett centralt licens-hanteringssystem. Det centrala licenshanteringssystemet beviljar pay- per-use-licenser till användaren när förfrågan har tagits emot och betalningsuppgifter har tagits.

Detta tillvägagångssätt har dock nackdelen att användaren måste vara ansluten till det centrala licenhanteringssystemet för att kunna beviljas en pay-per-use-licens. Således, precis som i fallet med licensmodulen, kan mjukvaran inte på ett enkelt sätt användas på mobila elektroniska enheter såsom en bärbar dator eller en personlig dataenhet.

Det finns därför ett behov av ett system och en metod för att förhindra obehörig åtkomst till elektronisk data som har ett helt nytt tillvägagångssätt och övervinner nackdelarna hos de konventionella teknikerna.

SAMMANFATTNING AV UPPFINNINGEN

Den aktuella uppfinningen tillhandahåller i det stora hela ett nytt system och en ny metod för att förhindra obehörig åtkomst till elektroniska data.

En aspekt hos den aktuella uppfinningen den aktuella uppfinningen tillhandahållas ett system och en metod för att förhindra obehörig åtkomst till elektroniska data lagrade på en elektronisk enhet. Ett bärbart licensmedium konfigureras för att kommunicera med den elektroniska enheten för lagring av licensdata. Licensdata används av den elektroniska enheten för att fastställa om åtkomst till elektroniska data ska beviljas. En registreringsinstans är konfigurerad för att kommunicera med den elektroniska enheten.

Registreringsinstansen har verifikationsdata för att bekräfta licensdata som lagras på licensmediet. Registreringsinstansen tillhandahåller uppdaterad licensdata till licensmediet.

Införlivning av den aktuella uppfinningen kan inkludera en eller flera av följande funktioner. Den elektroniska enheten kan bekräfta giltigheten hos licensmediet genom att jämföra licensdata med verifikationsdata på registreringsinstansen.

Licensmediet kan lagra ett meddelandesammanställning för licensdata som skapas genom att göra en hash för licensdata. Verifikationsdata kan inkludera en kopia av licensdatans meddelandesammanställning. Den elektroniska enheten kan bekräfta licensmediets giltighet genom att jämföra licensdatans meddelandesammanställning med kopian av licensdatans meddelandesammanställning i verifikationsdatan för registreringsinstansen.

Licensdatan meddelandesammanställning kan vara krypterat med en privat nyckel kopplad till registrerings-instansen. Den privata nyckeln kan vara en av flera privata nycklar som är kopplade till registreringsinstansen. Verifikationsdatan kan inkludera en kopia av det krypterade licensdata-meddelandesammanställning. Den elektroniska enheten kan bekräfta licensmediets giltighet genom att jämföra det krypterade licensdata-meddelandesammanställning med kopian av den krypterade licensdata-meddelandesammanställningen på registreringsinstansen.

Den elektroniska enheten kan bekräfta licensmediets giltighet genom att avkryptera licensdata-meddelandesammanställningen som läses från licensmediet med hjälp av en allmän nyckel kopplad till registreringsinstansen, vilket skapar en meddelandesammanställning genom att tillämpa en hash på licensdatan som läses från licensmediet och jämföra det avkrypterade meddelandesammanställningen med den genererade meddelandesammanställningen.

Den elektroniska enheten kan skicka registrerings-information till registreringsinstansen. Registrerings-informationen kan innehålla en slumpmässig identifierare som är kopplad till elektroniska data. Verifikations-data som lagras i registreringsinstansens databas kan inkludera en lista över behöriga identifierare som tillåter åtkomst till elektroniska data. Registreringsinstansen kan tillhandahålla uppdaterad licensdata till licensmediet när identifieraren som skickas tillsammans med registrerings-informationen överensstämmer med en av de behöriga identifierarna.

Licensmediet kan vara ett smartkort som har ett minne. Smartkortet kan också ha en mikroprocessor. Smartkortet kan kryptera ett första meddelandesammanställning som tas emot från registreringsinstansen med hjälp av en allmän nyckel som är kopplad till registreringsinstansen, generera ett andra meddelandesammanställning genom att tillämpa en hash på de uppdaterade licensdata som tas emot från registreringsinstansen och jämföra den första meddelandesammanställningen med den andra meddelandesammanställningen. Licensmediet kan också vara en minnessticka, ett skrivminne eller en datordisk (d.v.s. optisk, magnetisk eller elektronisk). Licensmediet kan ha ett minne installerat i en mobiltelefon som är eller inte är flyttbart.

Licensdatan kan inkludera förfallodata för licensmedium som avgörs av en konfigurerbar tidsperiod under vilken licensmediet är giltigt. Licensmediet förfalloperiod kan exempelvis vara trettio dagar.

Licensdatan kan inkludera förfallodata för en mjukvarulicens som fastställs av en konfigurerbar tidsperiod under vilken åtkomst till elektroniska data är tillåten. Mjukvarulicensens förfalloperiod kan exempelvis vara en dag eller trettio dagar.

Licensdatan kan inkludera ett säkerhetsförfallodatum för mjukvaran som avgörs av en konfigurerbar tidsperiod under vilken tillgång till elektroniska data tillåts. Säkerhetsförfalloperioden för mjukvaran kan t.ex. vara trettio dagar.

En annan aspekt av den aktuella uppfinningen tillhandahåller ett system och en metod för att förhindra obehörig åtkomst till elektronisk data som lagras på en elektronisk enhet. Ett bärbart licensmedium konfigureras för att kommunicera med den elektroniska enheten för lagring av licensdata. Licensdatan används för att fastställa om åtkomst ska beviljas till elektroniska data. En registreringsinstans konfigureras för att kommunicera med den elektroniska enheten. Registreringsinstansen har en första databas av verifikationsdata för verifiering av licensdata som lagras i en andra verifikationsdatabas. En licenshanterare konfigureras för att kommunicera med den elektroniska enheten och registreringsinstansen. Licenshanteraren har en andra databas med verifikationsdata för att verifiera licensdatan som lagras på licensmediet. Licenshanteraren tillhandahåller uppdaterad licensdata till licensmediet.

Införlivande av den aktuella uppfinningen kan inkludera en eller flera av följande funktioner. Den elektroniska enheten kan bekräfta licensmediets giltighet genom att jämföra licensdatan mot den andra databasen med verifikationsdata för licenshanteraren. Licenshanteraren kan bekräfta giltigheten för den andra databasen med verifikationsdata genom att jämföra den med den första databas med verifikationsdata för registreringsinstansen.

Licensmediet kan lagra ett licensdata-meddelandesammanställning som skapas genom att man tillämpar en hash för licensdatan. Den andra databasen med verifikationsdata kan inkludera en kopia av licensdata-meddelandesammanställning . Den elektroniska enheten kan bekräfta licensmediets giltighet genom att jämföra licensdata-meddelandesammanställningen med kopian av licensdata-meddelandesammanställning i den andra databasen med verifikationsdata för licenshanteraren.

Licensdata-meddelandesammanställning kan krypteras med en privat nyckel som är kopplad till registrerings-instansen eller licenshanteraren. Den privata nyckeln kan vara en av ett antal privata nycklar kopplade till registreringsinstansen eller licenshanteraren. Den andra databasen med verifikationsdata kan inkludera en kopia av den krypterade licensdata-meddelandesammanställningen.

Den elektroniska enheten kan bekräfta licensmediets giltighet genom att jämföra den krypterade licensdata-meddelandesammanställning med kopian av den krypterade licensdata-meddelandesammanställning i den andra databasen med verifikationsdata för licenshanteraren.

Den elektroniska enheten kan bekräfta licensmediets giltighet genom att avkryptera licensdata-meddelandesammanställningen som läses från licensmediet med hjälp av en allmän nyckel kopplad till registrerings-instansen, skapa en meddelandesammanställning genom att tillämpa en hash på licensdatan som läses från licensmediet och jämföra den krypterade meddelandesammanställningen med den genererade meddelandesammanställningen.

Licenshanteraren kan skicka platslicensregistrerings-information till registreringsinstansen. Platslicensregistreringsinformationen kan inkludera en slumpad identifierare som är kopplad till elektroniska data. Verifikationsdatan som lagras i registreringsinstansens databas kan inkludera en lista över behöriga identifierare som tillåter åtkomst till elektroniska data. Registreringsinstansen kan tillhandahålla uppdaterade verifikationsdata till licenshanteraren när den identifierare som skickas med registreringsinformationen överensstämmer med en av de behöriga identifierarna.

Licenshanteraren kan kommunicera med registreringsinstansen för att bekräfta att verifikationsdatan som lagras av licenshanteraren överensstämmer med verifikationsdatan som lagras av registreringsinstansen.

Dessa och andra föremål, funktioner och fördelar kommer att bli uppenbara genom följande beskrivning av den föredragna införlivandet av den aktuella uppfinningen.

KORT BESKRIVNING AV RITNINGARNA

Den aktuella uppfinningen kommer att bli lättare att förstå genom en detaljerad beskrivning av de föredragna införlivandena tillsammans med följande figurer.

BILD **1** är ett blockdiagram av ett system för skydd av licensierade elektroniska data som används av en klientdator.

BILD **2** visar ett smartkort med ytkontakter.

BILD **3** är ett blockdiagram av smartkortets inre mikrochip.

BILD **4** är ett blockdiagram av ett system för skydd av licensierade elektroniska data som används av en fjärrklientdator.

BILD **5** är ett blockdiagram av ett system för skydd av licensierade elektroniska data som används av ett klientdatanätverk.

BILD **6** är ett diagram av mjukvaruregistrering för ett enanvändarsystem.

BILD **7** är ett diagram av mjukvaruuppstart för ett enanvändarsystem.

BILD **8** är ett diagram av tillägg av en mjukvarulicens till en anställds smartkort i ett fleranvändarsystem.

BILD **9** är ett diagram av mjukvaruuppstart för en fast nodlicens i ett fleranvändarsystem.

BILD **10** är ett diagram av mjukvaruuppstart för en flytande licens i ett fleranvändarsystem.

DETALJERAD BERSKRIVNING AV DE FÖREDRAGNA INFÖRLIVNINGARNA

BILD **1** visar ett blockdiagram som i allmänna ordalag visar införlivandet av den aktuella uppfinningen. På BILD **1**, kan en persondator **100**, kallad klientenheten, konfigureras för att använda licensierad datormjukvara tillhandahållen av en tredjepartsförsäljare.

Självklart är inte den aktuella uppfinningen begränsad till att förhindra obehörig åtkomst till datormjukvara på persondatorer. Andra exempel på elektroniska enheter som använder licensierade elektroniska data inkluderar DVD-spelare, handhållna datorenheter, personliga dataenheter (PDA:er), cellulära eller personliga kommunikationssystem (PCS) telefoner, intelligenta enheter (t.ex. kylskåp, värme- och kylsystem), internetenheter m.m. Andra exempel på licensierade elektroniska data inkluderar datormjukvara, musik, filmer, e-böcker, konstverk, privilegierade data (såsom databaser, privilegierade publikationer och kommunikation), etc. Andra exempel på båda finns också.

I allmänna ordalag använder den aktuella uppfinningens skyddssystem en registreringsinstans **110** som avgör ifall en användare är behörig att ha åtkomst till en specifik del av elektroniska data. Så som det används häri hänvisar "åtkomst till elektroniska data" och dess derivat (t.ex. "komma åt elektroniska data") brett till alla typer av manipulation av elektroniska data, inklusive (men inte begränsat till) att installera, använda, kopiera, inmata, utmata, läsa, skriva, visa, spela, lagra, flytta, bearbeta, o.s.v. Registreringsinstansen **110** kan användas som en server i ett nätverk och drivas under kontroll av en mjukvaruskyddsadministratör.

Mjukvaruskyddsadministratören upprätthåller registreringsinstansen **110** i samarbete med säljaren av elektroniska data.

Som en del av ett sådant skyddssystem kan säljaren kräva installation av ett klientprogram som tillhandahålls av mjukvaruskyddsadministratören. Klientprogrammet som installeras på klientdatorn **100** kommunicerar med ett lagringsmedium för licensinformation **120**, hänvisat till som licensmediet, och registreringsinstansen **110**. Alternativt kan klientprogrammet vara inbäddat i elektroniska data

Och kan verkställas då elektroniska data ska kommas åt, istället för att installeras separat av användaren. Registreringsinstansen **110**, i sin tur, kommunicerar med säljaren **130** vilken upprätthåller en databas över giltiga licenser som utfärdats för elektroniska data.

Licensmediet **120** är en bärbar komponent som innehåller information gällande mjukvaran eller andra licensierade elektroniska data som användaren har behörig åtkomst till. När en användare söker åtkomst till en såld del av elektroniska data kommunicerar klientprogrammet med licensmediet **120** för att bekräfta att användaren är behörig att ha åtkomst till elektroniska data.

Generellt kan licensmediet **120** vara vilken typ av bärbar datalagringsenhet som helst som har ett unikt, oändringsbart serienummer eller annan sorts identifiering som kan skickas elektroniskt. Exempel inkluderar smartkort, minnesstickor, , kort med magnetremsa, disketter och andra borttagbara datorlagringsmedia. Licensmediet **120** och den elektroniska enheten som använder licensierade elektroniska data behöver inte ha en fast anslutning. En trådlös anslutning, d.v.s. en infraröd eller radiofrekvenslänk (RF) kan användas.

I vissa typer av elektroniska enheter kan licensmediet **120** konfigureras så att det inte är borttagbart, t.ex. i vissa typer av mobiltelefoner, handhållna datorenheter eller kontrollboxar för kabel-TV. Exempelvis så kan licensmediet vara ett internt RAM-minne som är installerat i mobiltelefonen. Det övervägs också om att uppfinningen kan inkludera stationära enheter som exempelvis kylskåp eller andra vitvaror som har ett licensmedium som inte är borttagbart.

I exemplet på BILD **1** används ett smartkort som licensmedium. Som visat på BILD **2** är ett smartkort **120** ett plastkort som innehåller ett mikrochip **300**. Kontakter **305** för mikrochipet **300** formas på kortets yta **120** för att tillhandahålla in- och utgående data och strömförsörjning.

Som visat på BILD **3** inkluderar mikrochipet **300** en central bearbetningsenhet (CPU) **310** som är kopplat till ett RAM-minne **315**, även om ett smartkort utan CPU också kan användas. RAM **315** används för att temporärt lagra information under bearbetningen samtidigt som kortet förses med ström. Ett ROM-minne (skrivskyddat) **320** lagrar permanent mikrochipets operativsystem. Ett raderbart omprogrammerbart skrivskyddat minne (EPROM) **325** lagrar applikationskod och data, såsom den licensinformation som tas upp ovan.

Åter med hänvisning till BILD **1**, klient programmet får åtkomst till smartkortet **120** med hjälp av en smartkortläsare **140** som är kopplad till klientdatorn **100**. Smartkortet **120** innehåller licensinformation som anger till klientprogrammet vilken mjukvara användaren har behörig åtkomst till. Licensinformationen kan även inkludera annan information, exempelvis tidsstämplar som anger när licensen för varje auktoriserad mjukvara förfaller.

Smartkortet kan vara ett dedicerat smartkort som är specifikt tillhandahållet för användning som licensmedium. Alternativt har ett allmänt smartkort andra funktioner, ett kreditkort kan exempelvis anpassa för att användas som licensmedium. I sådana fall skulle smartkortet fungera både för sitt ursprungliga syfte och som licensmedium.

Registreringsinstansen **110** är en fjärrserver som innehåller en licensdatabas som innehåller information för alla licensmedia **120** som givits behörighet av administratören för mjukvaruskydd av mjukvarans försäljare **130**. Klientprogrammet kommunicerar med registreringsinstansen **110** för att utföra Ett antal funktioner kopplade till skyddssystemets drift. Klientprogrammet kan exempelvis kommunicera med registreringsinstansen **110** med hjälp av Internet **150**.

Exempelvis så kan klientprogrammet verifiera giltigheten hos smartkortet **120** genom att kommunicera med registreringsinstansen **110**. Som ännu ett exempel kommunicerar klientprogrammet med registreringsinstansen **110** för att ändra smartkortets innehåll **120** för att lägga till, ta bort eller ändra användarens åtkomst till mjukvaran. Smartkortets innehåll **120** kan också ändras för att överföra en licens för åtkomst till mjukvaran från ett smartkort till ett annat eller för att uppdatera tidsstämplar som anger när den behöriga användningen av mjukvaran eller själva licensmediet upphör.

Som visat på BILD **4** behöver inte licensmediet och den elektroniska enheten finnas på samma plats. Licensmediet, t.ex. ett smartkort **120**, kan vara anslutet till användarens dator **160**, som i sin tur är ansluten till klientenheten **100** via Internet 150. Klientenheten **100** kan vara en fjärrserver som kör licensierade mjukvaror som värd för en ägd eller kommersiell databas som användaren är behörig att ansluta till.

Som ytterligare ett exempel kan klientenheten **100** vara en fjärrinternetserver som innehåller computer aided drafting (CAD)-filer, såsom byggnadsritningar. I sådana fall fungerar smartkortet **120** effektivt som en portvakt som tillåter behöriga användare, t.ex. arkitekter, byggare och entreprenörer, att få åtkomst till ritningarna.

Såsom visas på BILDA **5** kan mjukvaran vara licensierad till en användare i enlighet med en platslicens som tillåter ett antal användare på licensens plats att använda mjukvaran. En platslicens köps oftast av ett företag som har flera användare kopplat till ett lokalt områdesnätverk (LAN). I en platslicenskonfiguration kommunicerar klientprogrammet med en licenshanterare **200** som tillhandahålls på en server i användarnas LAN. Licenshanteraren **200**, i sin tur, kommunicerar med registreringsinstansen **110** via Internet **150**. En övertalig licenshanterare **210** kan tillhandahållas för ökad pålitlighet.

I tillägg till kommunikationen mellan klientprogrammet på klientdatorn **100** och licensmediet **120** och registreringsinstansen **110** som beskrivs ovan utför skyddssystemet även kommunikation mellan licensmediet **120** och mjukvaran.

Mjukvaran inkluderar applikationsprogrammeringsgränssnitt (API:er) som regelbundet låter mjukvaran få åtkomst till smartkortet för att säkerställa att det är installerat i läsaren. Mjukvaran läser också licensinformationen som smartkortet innehåller för att säkerställa att användarens licens är giltig och inte har förfallit eller dragits in. Om mjukvaran fastställer att användaren inte har en giltig licens kan avbryta eller stoppa driften, meddela användaren om situationen, ge användaren en möjlighet att rätta till situationen och/eller vidta andra åtgärder beroende på de instruktioner som försäljaren har inkluderat i mjukvaran.

Som vi tagit upp ovan kan det krävas att användaren installerar ett klientprogram som tillhandahålls med mjukvaruskyddsadministratören för att installera och registrera skyddad mjukvara. Detta kan göras med hjälp av en installationsguide som tillhandahålls av mjukvaruskyddsadministratören, d.v.s. ett program som kontrollerar installationsprocessen för mjukvaran. Installationsguiden kan vara inkluderas med försäljarens mjukvara på ett skrivskyddat kompakt skivminne (CD-ROM) eller så har den kanske redan har installerats på klientdatorn under en tidigare mjukvaruinstallation. Installationsguiden installerar klientprogrammet på klientdatorn.

När klientprogrammet har installerats fortsätter installationen och registreringen av den skyddade mjukvaran såsom visas på BILD 6. Den skyddade mjukvaran installeras på klientdatorn och användaren uppmanas att registrera den skyddade mjukvarna hos registreringsinstansen.

För att registrera mjukvaran måste användaren sätta i ett smartkort i en läsare ansluten till datorn och måste ha internetuppkoppling eller modem. Om dessa anslutningsalternativ inte finns tillgängliga eller om användaren inte vill registrera mjukvaran vid tiden för installationen kan användaren tillåtas att använda mjukvaran under en begränsad tid i testläge i enlighet med försäljarens licensvillkor.

Klientprogrammet läser data från smartkortet och skickar dem till registreringsinstansen tillsammans med en uppsättning registreringsinformation. Registreringsinstansen jämför först smartkortets data med motsvarande data som lagras i en databas för att bekräfta att smartkortet är giltigt. Registreringsinstansen jämför sedan registreringsinformationen med motsvarande data som lagras i en databas för att bekräfta att den nya mjukvaruregistreringen är behörig.

Smartkortets data som skickas till registreringsinstansen inkluderar en meddelandesammanställning som genererades genom att en hashfunktion utfördes på smartkortets data. Hashfunktionen tar en dataström av godtycklig längd och skapar en kod med fast längd, vilken kallas en meddelandesammanställning eller hash. Registreringsinstansen jämför meddelandesammanställningen till ett motsvarande inlägg i databasen för att fastställa att smartkortet är giltigt.

Hashfunktioner har följande egenskaper och anses allmänt vara kryptografiskt lämpliga, d.v.s. säkra. För det första måste hashfunktionen i huvudsak vara en envägsfunktion, så att när en meddelandesammanfattning tas emot så är det i stort sett omöjligt att fastställa originaldataströmmen. För det andra måste hashfunktionen producera en i stort sett unik meddelandesammanställning så att det är så gott som omöjligt att hitta två meddelanden som skapar samma meddelandesammanställning. Hashfunktioner som ofta används inkluderar: Message Digest 2 (MD2), Message Digest 4 (MD4), Message Digest 5 (MD5), the Secure Hash Algorithm (SHA) och Secure Hash Algorithm 2 (SHA- 2).

Registreringsinformationen som skickas till registreringsinstansen inkluderar den unika identifieraren för mjukvaran som ska registreras. Identifieraren kan bestå av ett serienummer och ett lösenord eller en lösenordsfras för att förhindra att en obehörig användare listar ut serienumren. Serienumret och lösenordet trycke på det CD-ROM-fodral i vilket mjukvaran distribueras. Alternativt kan identifieraren genereras från två orelaterade komponenter, t.ex. två slumpvalda ord som väljs ur en ordbok. Registreringsinstansen jämför identifieraren som mottogs tillsammans med registreringsinformationen mot en databas över giltiga identifierare som tillhandahålls av mjukvaruförsäljaren.

Registreringsinformationen som skickas till registreringsinstansen inkluderar även annan information, såsom ett produktnummer för mjukvaran som ska registreras, ett unikt smartkort-serienummer, ett smartkort-sekvensnummer. Registreringsinformationen inkluderar också förfalloperioder för smartkortet och mjukvarulicenser som tas upp ytterligare nedan.

Om registreringsinformation bekräftas av registreringsinstansen, skapas en ny registreringspost för den nyligen beviljade eller uppdaterade licensen för mjukvaran. Registreringsinstansen genererar nya smartkortsdata som visar dessa ändringar och skickar tillbaka dessa data till klientdatorn för att lagras på smartkortet.

Registreringsinstansen skickar också en hash med nya smartkortdata till klientdatorn. Hashen är krypterad

Med en privat nyckel som tillhör mjukvaruskyddsadministratören. Den krypterade hashen kan avkrypteras av alla som har motsvarande allmänna nyckel. Mjukvaruskyddsadministratören är dock den ende som kan generera en sådan krypterad hash. Således blir den krypterade hashen en digital signatur för mjukvaruskyddsadministratören.

Den privata nyckeln som använda av mjukvaruskyddsadministratören kan vara en i en uppsättning privata nycklar, t.ex. en uppsättning på 100 nycklar. Genom att använda en stor uppsättning privata nycklar blir det extra svårt att knäcka en specifik nyckel i ett set eftersom en ny nyckel kanske används för varje uppdatering.

Klientprogrammet får nya data och den krypterade hashen och lagrar dem på smartkortet. Varje gång det ansluts till smartkortet på det här sättet utför smartkortet en hashjämförelse genom att använda sin interna processor för att förhindra obehöriga ändringar av smartkortets data.

För att göra hashjämförelsen avkrypterar smartkortets processor den hash som mottagits från registreringsinstansen med hjälp av en allmän nyckel. Smartkortet genererar sedan en hash för nya data. Den genererade hashen och den avkrypterade hashen jämförs för att säkerställa att nya data kom från registreringsinstansen.

De nya smartkortsdata som skickats av registreringsinstansen inkluderar också ett nytt smartkort-sekvensnummer, ett nytt förfallodatum för smartkortet, förfallodatum för mjukvarulicens och förfallodatum för mjukvarusäkerhet.

Smartkortets sekvensnummer låter registreringsinstansen spåra uppdateringar för smartkortet. Exempelvis så kan sekvensnumret vara ett n-bitord (där n är ett heltal) som ökar varje gång smartkortet uppdateras. Denna funktion låter registreringsinstansen upptäcka obehörig åtkomst till smartkortet.

Mjukvarulicensens förfallodatum fastställs av en konfigurerbar tidsperiod under vilken licensen är giltig baserat på licensavtalet med användaren. Exempelvis så kan förfalloperioden för mjukvarulicensen vara en timme, en dag, trettio dagar, ett år eller någon annan period som överenskommits.

Varje mjukvarulicens kan ha en motsvarande förfalloperiod för mjukvarusäkerhet som fastställs av en konfigurerbar tidsperiod inom vilken användaren måste återkoppla till registreringsinstansen för att förnya mjukvarulicensen. Förfalloperioden för mjukvarans säkerhet kan fastställas av säljaren beroende på säkerhetskraven och kan vara vilken som helst önskad tidslängd.

Smartkortets förfallodatum fastställas av en konfigurerbar tidsperiod under vilken smartkortet kommer att fungera. Smartkortets förfalloperiod kan fastställas av mjukvaruskyddsadministratören baserat på säkerhet och övriga krav och kan vara vilken önskad tidslängd som helst, t.ex. 30 dagar. Smartkortets förfalloperiod kan ställas in så att den är densamma som den kortaste förfalloperioden för mjukvarusäkerhet som lagras på kortet.

Smartkortet måste uppdateras av registreringsinstansen inom smartkortets förfalloperiod och mjukvarusäkerhetens förfalloperiod om användaren ska ha oavbruten åtkomst till mjukvaran. Således, om ett smartkort skulle tappas bort eller stjälas, skulle en obehörig användare endast kunna använda smartkortet under den kvarvarande tiden för den kortaste av dessa förfalloperioder. Dessutom kan det borttappade eller stulna kortet avaktiveras nästa gång den elektroniska enheten kommunicerar med registreringsinstansen.

Nya smartkortsdata som skickas av registreringsinstansen kan inkludera en behörighetsnyckel för mjukvaran, till exempel en hash av produktens förfallodatum och produktnummer. Behörighetsnyckeln anger till smartkortet

att användaren är behörig att använda mjukvaran. Alternativt, om lagringsutrymme och tid står högt i kurs, kan en binär flagga användas som behörighetsnyckel.

Som angivet ovan kan nya data som lagras på smartkortet tillåta användaren att använda mjukvaran under en konfigurerbar tidsperiod, t.ex. 30 dagar, som angivet av mjukvarulicensen och mjukvarans säkerhetsförfallodatum. Mjukvaran kan under dessa tidsperioder användas utan ytterligare kommunikation med registreringsinstansen under förutsättning att smartkortet finns närvarande.

Mjukvarulicensens förfalloperiod kan användas för att tillämpa en korttidslicens. Exempelvis kan en mjukvarulicens köpas dag för dag. I ett sådant fall låter användaren mjukvaran vara installeras på sin dator, men ansluter endast till registreringsinstansen när mjukvaran behövs. Vid anslutningen till registreringsinstansen får användaren nya smartkotdata som har ett förfallodatum för mjukvarulicensen på en dag.

För att ta bort en registrerad mjukvaruprodukt från ett smartkort kan användaren köra ett avinstallationsprogram, t.ex. Windows™ kontrollpanel-applet. Avinstallationsprogrammet ansluter till registreringsinstansen som modifierar databasen för behöriga mjukvarulicenser. Serienumret på den borttagna mjukvaran kan återgå till en databas över behöriga serienummer så att en annan användare kan registrera det, eller så kan serienumret ges en inaktiv status tills det återaktiveras.

Registreringsinstansen skickar ny smartkortdata till användaren och visar borttagandet av mjukvarulicensen. Istället för att ta bort inlägget på smartkortet kan registreringsinstansen ändra mjukvarulicensens förfallodatum till ett datum som redan varit. Således kommer smartkortets data visa att produkten varit licensierad till smartkortet, men inte längre är giltig.

Under mjukvarans registreringsprocess kommer användaren att tillfrågas om automatisk uppdatering av smartkortets data ska tillåtas när en internetanslutning upptäcks. Om användaren tillåter automatiska uppdateringar kommer en mjukvarumodul, såsom en daemon (d.v.s. en process som körs i bakgrunden och utför en specifik uppgift vid förbestämda tidpunkter eller som svar på vissa händelser), kunna användas för att kontinuerligt bevaka om internetanslutning finns och uppdatera smartkortets data i bakgrunden. Alternativt startar klientprogrammet en bakgrundsuppgift för att utföra dessa funktioner på ett liknande sätt som Microsoft Critical Update Manager. Automatisk uppdatering av smartkortets data skulle låta användaren ha den maximala förfalloperioden för mjukvarulicensen, t.ex. trettio dagar, för all licensierad mjukvara.

Under en automatisk uppdatering av smartkortet överförs smartkortdata, inklusive den krypterade hashen av smartkortets data och sekvensnumret till registreringsinstansen. Smartkortets data inkluderar även alla registrerade produkter som har lagts till på kortet sedan den senaste uppdateringen, såsom testanvändningsinstallationer. De nya produktposterna kan också inkludera nya mjukvaruinstallationer till vilka försäljaren tillåter tillfällig registrering utan anslutning till registreringsinstansen. Närvaron av nya produkter på smartkortet kan upptäckas genom att man undersöker ett fält över senast registrerade på smartkortet eller ett binärt fält för varje registrerad produkt.

Vid mottagning av smartkortsdata kontrollerar registreringsinstansen en databas med verifikationsdata för att bekräfta att smartkortets data är. Databasen kan exempelvis vara en logisk databas som lagras separat eller med andra data i en annan logisk eller fysisk databas.

Registreringsinstansen bekräftar sådana saker som smartkortets sekvensnummer och smartkortet förfallodatum. Dessutom bekräftas den krypterade hashen av smartkortets data genom att den avkrypteras med en allmän nyckel.

Efter bekräftelserna av smartkortets data lagrar registreringsinstansen smartkortets nya data i sin databas. Registreringsinstansen genererar nya smartkortdata för att uppdatera förfallodatum och sekvensnummer för smartkortet och genererar en ny krypterad hash av dessa nya smartkortdata. Nya smartkortdata lagras på kortet och en bekräftelse skickas till registreringsinstansen.

Som vi tog upp ovan, om användaren inte har någon internetuppkoppling eller modem eller inte vill registrera mjukvaran vid installationstillfället kan användaren få lov att använda mjukvaran under en begränsad tid i testläge i enlighet med försäljarens licensregler.

Om försäljarens licensregler tillåter testanvändning så kommer klientprogrammet att konfigureras för att etablera en testanvändning för användaren. Klientprogrammet kontrollerar först det installerade smartkortet för att avgöra om det redan finns en testpost för mjukvaran i fråga. En testpost läggs in på smartkortet första gången användaren beviljas en testanvändning av mjukvaran och lagras på smartkortet för gott. Således kan klientprogrammet avgöra om användaren tidigare har beviljats en testanvändning och, om så är fallet, kan klientprogrammet inte bevilja fler testanvändningar.

När en testpost har gjorts utförs en ny hash på nya smartkortdata, inklusive testposten och lagras på smartkortet. Således kan testposten inte tas bort utan att smartkortet ogiltigförklaras.

Om användaren inte tidigare har beviljats en test för mjukvaran görs en testpost på smartkortet. Testposten inkluderar en konfigurerbar tidsgräns för testanvändningen, t.ex. 30 dagar. Användaren kan då använda mjukvaran under testperioden.

Om användaren senare har åtkomst till en internetanslutning så kan testversionen konverteras till en full licens om korrekta registreringsförfaranden utförs eller om registreringsinstansen har mottagit auktorisering från försäljaren. Som vi talat om ovan kan mjukvaran också konfigureras för att fråga användaren om en automatisk uppgradering önskas då internetuppkoppling hittas.

För att använda den registrerade mjukvaran måste användaren sätta i ett smartkort som innehåller giltig licensinformation i smartkortläsaren på klientdatorn, d.v.s. ett smartkort som har förberetts på det sätt som beskrivs ovan. Som BILD 7 visar, när användaren försöker att aktivera mjukvaran, kontrollerar klientdatorn för att se om ett smartkort är isatt. Om inte så uppmanas användaren att sätta i smartkortet.

Klientprogrammet läser innehållet på smartkortet och bekräftar att det inte har manipulerats. Klientprogrammet hämtar sedan licensinformationen för den specifika mjukvaran. Licensinformationen låter klientprogrammet avgöra om användaren är behörig att använda mjukvaran och att den auktoriserade användningsperioden eller provperioden inte har förfallit.

Klientprogrammet kan använda den krypterade hashen för att upptäcka smartkortet har ändrats. Klientprogrammet avkrypterar meddelandesammanställningen som lagras på smartkortet genom att använda en allmän nyckel. Klientprogrammet genererar sedan en meddelandesammanställning för smartkortets data med hjälp av en hashfunktion. Klientprogrammet jämför sedan den genererade meddelandesammanställningen med den avkrypterade meddelandesammanställningen. Om dessa meddelandesammanställningar överensstämmer så har smartkortet inte ändrats. Denna process låter klientprogrammet verifiera smartkortets giltighet utan att kommunicera med registreringsinstansen.

När verifikationen är genomförd tillåter klientprogrammet användning av mjukvaran. Under användningen kontrollerar mjukvaran regelbundet efter närvaron av ett giltigt smartkort med hjälp av applikationsprogrammeringsgränssnitt (API:er) i intervaller som fastställs av mjukvaruförsäljaren. API:erna tillhandahålls av mjukvaruskyddsadministratören och kan tillämpas som dynamiskt länkade bibliotek (DLL:er).

För att förhindra manipulering kan DLL:erna signeras så att de kan valideras. Om det fastställs att modulerna har manipulerats kommer mjukvaran att sluta fungera tills dess att dessa moduler har bytts ut.

Tidsstämplar kan lagras på smartkortet när det kontrolleras av API:erna. Tidsstämplarna används för att förhindra en användare från att återställa systemklockan för att bibehålla en registrering efter mjukvarulicensens förfallodatum.

Åter med hänvisning till BILD **5**, en platslicens kan köpas av ett företag för att möjliggöra att mjukvaran kan användas av flera användare i ett LAN. Antalet användare fastställs vid köptillfället. Platslicenshållar-LAN inkluderar en licenshanterare **200**, som också kan vara LAN-server.

Licenshanteraren **200** fungerar som en mellanhand mellan klientdatorn **100** och registreringsinstansen **110**. Exempelvis så kommunicerar licenshanteraren **200** med registreringsinstansen **110** för att registrera licensen. Vanligtvis så har säljaren **130** av platslicensen överfört information gällande en ny platslicens till registreringsinstansen **110** före registreringen. Licenshanteraren **200** registrerar platslicensen via överföring till registreringsinstansen **110** av det serienummer/lösenord som tillhandahålls med mjukvaran.

Alternativt kan registreringen göras på ett sätt som liknar installationen för en enskild användare som beskrivs ovan. I sådana fall installerar företagets licensadministratör, som vanligen också är LAN-administratör, den platslicensierade mjukvaran. En installationsguide installerar ett licenshanteringsprogram som bekräftar giltigheten hos det isatta smartkortet **120**. Licenshanteringsprogrammet kommunicerar också med registreringsinstansen **110** för att verifiera innehållet på smartkortet **120** och registrera platslicensen.

Licenshanteraren 120 upprätthåller en databas över all installerade platslicenserad mjukvara i LAN:et. Platslicensdatabasen synkroniseras regelbundet med en motsvarande databas hos registreringsinstansen **110**. Platslicensdatabasen inkluderar information gällande antalet fasta noder och flytande licenser.

Fasta nodlicenser tilldelas specifika individer, t.ex. en anställd på ett företag som har en platslicens. När den fasta nodlicensen tilldelas finns det en licens mindre tillgänglig för företaget. Licenshanteraren upprätthåller poster i platslicensdatabasen för var och en av de tilldelade fasta nodlicenserna.

Flytande licenser låter ett bestämt antal anställda använda mjukvaran samtidigt, en ytterligare licens blir tillgänglig för andra anställda. Licenshanteraren upprätthåller regelbundet en lista över aktuella användare för att fastställa att antalet användare inte överskrider den flytande licensens totala antal.

Som beskrivet ovan kommunicerar licenshanteraren **200** med registreringsinstansen **110** för att registrera den platslicensierade mjukvaran och upprätthåller platslicensdatabas. Dessutom, som BILD **8** visar, används licenshanteraren av företagets licensadministratör för att skapa och ändra smartkort som tilldelas varje anställd. Smartkorten programmeras med krypterad licensinformation som anger vilken platslicensierade mjukvara som den anställde har behörighet för.

Licensadministratören sätter i ett nytt eller befintligt smartkort **120** i en smartkortläsare **140** ansluten till licensadministratörens dator **100**, som är ansluten till LAN-servern/licenshanteraren **200**. Licensadministratörens dator **100** kommunicerar med licenshanteraren **200** för att leta upp motsvarande lagrade data eller skapa en ny post.

Om smartkortet **120** är till en vald befintlig anställd kommer licenshanteraren **200** att verifiera innehållet på smartkortet **120** och verifiera att smartkortet **120** tillhör den valde anställde. Licenshanteraren **200** kommunicerar sedan med registreringsinstansen **110** för att verifiera smartkortets giltighet **120** med hjälp av motsvarande data som lagras i registreringsinstansens databas.

När smartkortets giltighet **120** har verifierats kan licensadministratören välja nya licenser från de tillgängliga platslicenserna att lägga till på den anställdes kort **120**. Licenshanteraren **200** genererar ny licensinformation för smartkortet **120** och överför den till registreringsinstansen **110**. Registreringsinstansen **110** skickar tillbaka ny information till smartkortet **120**, som skrivs på kortet **120** av smartkortläsaren **140**.

För att använda den registrerade mjukvaran måste användaren sätta i ett smartkort **120** som innehåller giltig licensinformation i smartkortläsaren **140** på klientdatorn **100**, d.v.s. ett smartkort som har förberetts på det sätt som anges ovan. Som visas på BILD **9**, när en användare som har en fast nodplatslicens försöker att aktivera mjukvaran så kontrollerar klientdatorn **100** för att se om ett smartkort **120** är isatt. Om inte så uppmanas användaren att sätta i smartkortet **120**.

Klientprogrammet på klientdatorn **100** läser och verifierar smartkortets **120** giltighet för att fastställa att det inte har manipulerats. Verifieringsprocessen beskrivs mer detaljerat nedan. Klientprogrammet hämtar sedan licensinformationen för den specifika mjukvaran. Licensinformationen låter klientprogrammet verifiera att användaren är behörig att använda mjukvaran och att den auktoriserade användningsperioden eller testperioden inte har förfallit.

Klientprogrammet på klientdatorn **100** kommunicerar sedan med licenshanteraren **200** för att verifiera att användaren har en giltig fast nodlicens. Om användaren inte har en fast nodlicenspost i licensdatabasen som lagras av licenshanteraren **200** kan licenshanteraren **200** kontrollera om det finns en tillgänglig flytande licens, som tas upp mer i detalj nedan. Om varken en fast nodlicens eller en flytande licens är tillgänglig kommer användaren inte att verifieras. Denna konfigurering låter licenshanteraren **200** kontrollera tilldelningen av fasta nodlicenser utan att ansluta till registreringsinstansen **110**.

När verifieringen är genomförd tillåter klientprogrammet att mjukvaran använda. under användningen kan mjukvaran regelbundet omverifiera smartkortet genom att använda API:er i intervaller som fastställs av mjukvaruförsäljaren.

På samma sätt, så som visas på BILD **10**, när en användare med en flytande platslicens försöker att aktivera mjukvaran så kontrollerar klientdatorn **100** för att se om ett smartkort **120** är isatt. Om inte så uppmanas användaren att sätta i smartkortet **120**.

Klientprogrammet på klientdatorn **100** läser och verifierar giltigheten hos innehållet på smartkortet **120** för att säkerställa att det inte har manipulerats. Klientprogrammet hämtar sedan licensinformationen för den specifika mjukvaran.

Klientprogrammet på klientdatorn **100** kommunicerar sedan med licenshanteraren **200** för att fastsälla om en flytande licens finns tillgänglig. Om en flytande licens är

Tillgänglig så kommer den att reserveras för användaren, d.v.s. att antalet tillgängliga licenser minskar med en. Denna konfigurering låter licenshanteraren **200** kontrollera tilldelningen av flytande licenser utan att ansluta till registreringsinstansen **110**.

När verifieringen är genomförd tillåter klientprogrammet att mjukvaran används. Under användningen kan mjukvaran regelbundet omverifiera smartkortet med hjälp av API:er i intervaller som fastställs av mjukvaruförsäljaren. När användaren stänger ner mjukvaran låter klientdatorn licenshanteraren släppa den flytande licensen till andra användare.

En anställd kanske vill använda den registrerade mjukvaran på en dator som inte är anslutet till det lokala nätverket, t.ex. en laptop eller en hemdator. I sådana fall kommer inte klientprogrammet kunna kommunicera medlicenshanteraren för att verifiera att användaren har en giltig fast nodlicens eller att en flytande licens finns tillgänglig, vilket tas upp ovan. Den anställdes smartkort måste därför ändras av licenshanteraren för att tillåta användning av den registrerade mjukvaran på annan plats.

För en fast nodlicens skapar licenshanteraren en post på den anställdes smartkort som tillåter användning mjukvaran under en licensperiod, t.ex. 30 dagar. Under denna period kan den anställde använda mjukvaran utan att ansluta till licenshanteraren för verifiering.

För en flytande licens skapar licenshanteraren en post på den anställdes smartkort som tillåter användning av mjukvaran under en licensperiod, t.ex. 30 dagar, och reserverar en flytande licens. Under denna period kan den anställde använda mjukvaran utan att ansluta till licenshanteraren för verifiering. De andra anställda kommer dock inte ha åtkomst till denna flytande licens under den här perioden oavsett om den flytande licensen faktiskt används eller inte av den anställde som är på en annan plats.

Den anställde kan koppla upp sig mor det lokala nätverket då denne befinner sig på en annan plats, exempelvis för att kolla sin e-post. Vid anslutningen till det lokala nätverket kan licenshanteraren automatiskt uppdatera den anställdes smartkort för att starta om licensperioden. Således, om en anställd kontrollerar mer frekvent än licensperioden kan mjukvaran användas från en annan plats på obestämd tid.

När en användare får ett nytt smartkort så måste det registreras hos registreringsinstansen innan licensinformation lagras på det. Registreringen görs med hjälp av en registreringsguide på klientdatorn.

Registreringsguiden kan installeras automatiskt under installationen av den första skyddade mjukvaruprodukten på ett liknande sätt som installationen av klientprogrammet som tas upp ovan. Alternativt så kan registreringsguiden laddas ner från Internet, sampackas med en smartkortläsare, eller inkluderas i operativsystemet.

Under registreringen av smartkortet uppmanar registreringsguiden användaren att ange ett antal frågor och svar som troligen endast användaren känner till. Dessa frågor och svar krypteras med hjälp av en privat nyckel och skickas till registreringsinstansen tillsammans med kortets serienummer. Denna information kan användas under mjukvaruregistreringen och användas för att bekräfta att användaren faktiskt är ägare till smartkortet.

Smartkortets serienummer kan lagras på klientdatorn, t.ex. i registret. Om användaren glömmer eller tappar bort serienumret så kan användaren köra en applet för att återfå smartkortets serienummer från registret. Applet kan även ange vilka mjukvaruprodukter som finns registrerade på smartkortet.

Användaren kommer att instrueras att förvara smartkortets serienummer på en säker plats för att underlätta ersättning av kortet

Om det tappas bort, skadas eller stjäls. Om användaren inte vet smartkortets serienummer eller inte har åtkomst till klientdatorn kan användaren kontakta försäljaren av mjukvaruprodukten som är licensierad till smartkortet. Försäljaren kan tillhandahålla mjukvarans serienummer som kan användas av registreringsinstansen för att leta reda på smartkortets serienummer.

Om ett smartkort tappas bort eller stjäls kan användaren ringa ett gratisnummer eller använda Internet för att skicka nödvändig information till registreringsinstansen eller försäljaren för att få den licens som är lagrad på det gamla kortet, inklusive test, överförd till ett nytt kort. Det gamla kortet inaktiveras då i registreringsinstansens databas.

Om en obehörig användare försöker att förnya licenser på det gamla smartkortet genom att ansluta till registreringsinstansen så kommer det gamla smartkortet att inaktiveras. Om det fastställs att det gamla smartkort tilldelades nyligen så kan licensperioden för mjukvaruprodukterna förkortas på det nya smartkortet för att förhindra upprepade byten av smartkort.

Det uppskattas att var och en av de tillämpningar som tas upp ovan ger ett nytt system och metod för att förhindra obehörig åtkomst till elektroniska data som når de ovan angivna målen för den aktuella uppfinningen.

Det uppskattas också att eftersom licensmediet kan innehålla licenser från flera olika försäljare så låter systemet användaren få åtkomst till data från flera olika försäljare utan att behöva flera olika nycklar eller åtkomstenheter.

Det uppskattas också att eftersom licensmediet är kopplat till en specifik användare istället för en specifik elektronisk enhet så kan användaren få åtkomst till licensierade elektroniska data genom att använda en rad olika elektroniska enheter, t.ex. på en hemdator och en laptop.

Det uppskattas också att eftersom licensmediet kan lagra licensdata för elektroniska data från flera olika försäljare så kan användaren enkelt nå alla de data för vilka användaren är licensierad med hjälp av ett enda licensmedium.

Det uppskattas också att eftersom licensmediet är bärbart så kan systemet användas på alla datorer som har förmågan att läsa licensmediet. Således kan skyddade elektroniska data nås av innehavaren av licensmediet på en hemdator, bärbar dator, handdator, m.m.

Det uppskattas också att eftersom licensmediet tillåter åtkomst till skyddade elektroniska data under en konfigurerbar tidsperiod så kan användaren få åtkomst till data utan att ansluta till registreringsinstansen under denna tidsperiod. Således krävs inte en fast anslutning till registreringsinstansen eller Internet.

Det uppskattas också att eftersom licensmediet tillåter åtkomst till skyddade elektroniska data under en konfigurerbar tidsperiod så kan försäljaren erbjuda korttidslicenser, t.ex. veckovis, dagligen, timvis, etc.

Det uppskattas också att eftersom ett smartkort har en intern processor så kan det utföra krypterings- och hashfunktioner. Således kan smartkortet avkryptera en mottagen hash och jämföra den med en internt genererad hash av smartkortets data. Denna jämförelse låter smartkortet avgöra om mottagna data kommer från en behörig källa och således förhindra obehörig modifiering av smartkortets data.

Då den aktuella uppfinningen har beskrivits utifrån vad som för närvarande anses vara föredragna tillämpningar ska det förstås att uppfinningen inte är

Begränsad till de angivna tillämpningarna. Tvärtom är uppfinningen avsedd att täcka en rad modifieringar och motsvarande upplägg inkluderade i tanken och omfattningen hos de bifogade yrkandenpunkterna.

Det som yrkas:

1. Ett system för att förhindra obehörig åtkomst till elektroniska data på en elektronisk enhet, systemet består av:

Ett bärbart licensmedium konfigurerat för att kommunicera med den elektroniska enheten och lagra licensdata, licensdatan konfigureras för att användas av den elektroniska enheten för att fastställa om den ska tillåta åtkomst till elektroniska data; och

en registreringsinstans konfigurerad för att kommunicera med den elektroniska enheten, registreringsinstansen har verifikationsdata för att verifiera licensdatan som lagras licensmediet,

vari registreringsinstansen tillhandahåller uppdaterade licensdata för licensmediet.

2. Ett system i enlighet med punkt **1**, vari den elektroniska enheten är konfigurerad för att verifiera giltigheten hos licensmediet genom att jämföra licensdatan med verifikationsdatan .

3. Ett system i enlighet med punkt **1**, vari licensmediet är konfigurerat för att lagra en licensdata-meddelandesammanställning skapad genom användning av en hash av licensdatan.

4. Ett system i enlighet med punkt **3**, vari verifikationsdatan består av en kopia av licensdata-meddelandesammanställning .

5. Ett system i enlighet med punkt **4**, vari den elektroniska enheten är konfigurerad för att verifiera giltigheten hos licensmediet genom att jämföra licensdata-meddelandesammanställning med kopian av licensdata-meddelandesammanställningen i verifikationsdatan .

6. Ett system i enlighet med punkt **3**, vari licensdata-meddelandesammanställning krypterad med en privat nyckel kopplad till registreringsinstansen.

7. Ett system i enlighet med punkt **6**, vari den privata nyckeln är en av ett flertal privata nycklar kopplade till registreringsinstansen.

8. Ett system i enlighet med punkt **6**, vari verifikationsdatan består av en kopia av den krypterade licensdata-meddelandesammanställningen.

9. Ett system i enlighet med punkt **8**, vari den elektroniska enheten är konfigurerad för att verifiera giltigheten hos licensmediet genom att jämföra den krypterade licensdata-meddelandesammanställningen med kopian av den krypterade licensdata-meddelandesammanställningen i verifikationsdatan .

10. Ett system i enlighet med punkt **6**, vari den elektroniska enheten är konfigurerad för att verifiera giltigheten hos licensmediet genom att:

Avkryptera licensdata-meddelandesammanställningen som läses från licensmediet med en allmän nyckel kopplad till registreringsinstansen;

Genererar en meddelandesammanställning genom att utföra en hash på licensdatan som läses från licensmediet; och

Jämföra den avkrypterade meddelandesammanställningen med den genererade meddelandesammanställningen.

11. Ett system i enlighet med punkt **1**, vari den elektroniska enheten är konfigurerad för att skicka registreringsinformation till registreringsinstansen.

12. Ett system i enlighet med punkt **11**, vari registreringsinformationen består av en slumpad identifierare kopplad till elektroniska data.

13. Ett system i enlighet med punkt **12**, vari verifikationsdatan består av en lista behöriga identifierare som tillåter åtkomst till elektroniska data.

14. Ett system i enlighet med punkt **13**, vari registreringsinstansen är konfigurerad för att tillhandahålla uppdaterade licensdata till licensmediet när identifieraren som skickas med registreringsinformationen överensstämmer med en av de behöriga identifierarna.

15. Ett system i enlighet med punkt **1**, vari licensmediet består av ett smartkort som har ett minne.

16. Ett system i enlighet med punkt **15**, vari smartkortet har en mikroprocessor.

17. Ett system i enlighet med punkt **15**, vari smartkortet är konfigurerat för att avkryptera en första meddelandesammanställning som mottas från registreringsinstansen med hjälp av en allmän nyckel kopplad till registreringsinstansen, för att generera en andra meddelandesammanställning genom att utföra en hash på uppdaterad licensdata mottagen från registreringsinstansen, och jämföra den första meddelandesammanställningen med den andra meddelandesammanställningen.

18. Ett system i enlighet med punkt **15**, vari licensdatan består av ett sekvensnummer ger registreringsinstansen ett antal gånger som smartkortet har använts.

19. Ett system i enlighet med punkt **1**, vari licensmediet är en minnessticka.

20. Ett system i enlighet med punkt **1**, vari licensmediet är ett RAM-minne.

21. Ett system i enlighet med punkt **1**, vari licensmediet består av ett installerat minne på en mobiltelefon.

22. Ett system i enlighet med punkt **21**, vari licensmediet inte är borttagbart från mobiltelefonen.

23. Ett system i enlighet med punkt **1**, vari licensmediet är en datordisk.

24. Ett system i enlighet med punkt **23**, vari datordisken är en optisk disk.

25. Ett system i enlighet med punkt **23**, vari datordisken är en magnetisk disk.

26. Ett system i enlighet med punkt **23**, vari datordisken är en elektronisk disk.

27. Ett system i enlighet med punkt **1**, vari licensdatan består av ett förfallodatum för ett licensmedium genom en konfigurerbar tidsperiod under vilken licensmediet är giltigt.

28. Ett system i enlighet med punkt **1**, vari licensdatan består av ett förfallodatum för mjukvarulicensen fastställt av en konfigurerbar tidsperiod under vilken åtkomst till elektroniska data är tillåten.

29. Ett system i enlighet med punkter **27** eller **28**, vari licensmediets förfalloperiod är inställd till den kortaste mjukvarulicens-förfalloperioden för licensdatan.

30. Ett system i enlighet med punkt **1**, vari licensdatan består av ett mjukvarusäkerhets-förfallodatum fastställt av en konfigurerbar tidsperiod under vilken åtkomst till elektroniska data är tillåten

31. Ett system i enlighet med punkt **1**, vari licensmediet är konfigurerat för att kommunicera med den elektroniska enheten via en fast anslutning.

32. Ett system i enlighet med punkt **1**, vari licensmediet är konfigurerat för att kommunicera med den elektroniska enheten via en trådlös anslutning.

33. Ett system i enlighet med punkt **1**, vari licensmediet är konfigurerad för att kommunicera med den elektroniska enheten via ett nätverk.

34. Ett system i enlighet med punkt **33**, vari nätverket är Internet.

35. Ett system för att förhindra obehörig åtkomst till elektroniska data på en elektronisk enhet, systemet består av:

Licensdata-lagringsmedel konfigurerade för att kommunicera med den elektroniska enheten, licensdata konfigurerad för att användas av den elektroniska enheten för att fastställa om åtkomst till elektroniska data ska tillåtas; och

Registreringsauktoriseringsmedel konfigurerade för att kommunicera med den elektroniska enheten, registreringsauktoriseringsmedel att ha verifieringmedel för att verifiera licensdatan som är lagrad på licensmediet,

Vari registreringsauktoriseringsmedel är konfigurerad för att tillhandahålla uppdaterad licensdata till licensdatans lagringsmedel.

36. Ett system för att förhindra obehörig åtkomst till elektroniska data på en elektronisk enhet, systemet består av:

ett smartkort konfigurerat för att kommunicera med den elektroniska enheten och konfigurerat för att lagra licensdata, licensdata konfigurerad för att användas av den elektroniska enheten för att fastställa om åtkomst till elektroniska data ska tillåtas; och

en registreringsserver konfigurerad för att kommunicera med den elektroniska enheten, registreringsservern har verifikationsdata för att verifiera licensdatan som är lagrad på Smartkortet,

vari registreringsservern är konfigurerad för att tillhandahålla uppdaterad licensdata till smartkortet.

37. En registreringsinstans för att förhindra obehörig åtkomst till elektronisk data på en elektronisk enhet, registreringsinstansen består av:

medel för att kommunicera med den elektroniska enheten; och verifikationsdata för verifiering av licensdata lagrat på ett bärbart licensmedium som är konfigurerat för att kommunicera med den elektroniska enheten,

vari licensdatan används av den elektroniska enheten för att fastsälla om åtkomst till elektroniska data ska tillåtas, och

registreringsinstansen är konfigurerad för att tillhandahålla uppdaterad licensdata till licensmediet.

38. Ett smartkort för att förhindra obehörig åtkomst till elektronisk data på en elektronisk enhet, smartkortet består av:

medel för att kommunicera med den elektroniska enheten;

ett minne för lagring av data mottagen från kommunikationsmedlet; och

licensdata lagrad i minnet, licensdatan är konfigurerad för att användas av den elektroniska enheten för att fastsälla om åtkomst till elektroniska data ska tillåtas,

vari licensdatan hr verifierats av verifieringsdata stored på en registreringsserver som är konfigurerad för att kommunicera med den elektroniska enheten, och

smartkortet är konfigurerat för att ta emot tillhandahåller uppdaterad licensdata från registreringsservern.

39. Ett system för att förhindra obehörig åtkomst till elektroniska data på en elektronisk enhet, systemet består av:

ett bärbart licensmedium konfigurerat för att kommunicera med den elektroniska enheten och konfigurerat för att lagra licensdata, licensdatan är konfigurerad för att användas för att fastsälla om åtkomst till elektroniska data ska tillåtas;

en registreringsinstans med en första verifikationsdatabas för verifiering av licensdata som lagras i en andra verifikationsdatabas; och

en licenshanterare konfigurerad för att kommunicera med den elektroniska enheten och registreringsinstansen, licenshanteraren innehåller den andra verifikationsdatabasen för verifiering av licensdatan som lagras på licensmediet,

vari registreringsinstansen är konfigurerad för att tillhandahålla uppdaterad verifikationsdata för licenshanterarens andra verifikationsdatabas , och

licenshanteraren är konfigurerad för att tillhandahålla uppdaterad licensdata till licensmediet.

40. Ett system i enlighet med punkt **39**, vari den elektroniska enheten är konfigurerad för att verifiera giltigheten hos licensmediet genom att jämföra licensdatan med den andra verifikationsdatabasen.

41. Ett system i enlighet med punkt **39**, vari licenshanteraren är konfigurerad för att verifiera giltigheten hos den andra verifikationsdatabas genom att jämföra den med den första verifikationsdatabas.

42. Ett system i enlighet med punkt **39**, vari licensmediet är konfigurerat för att lagra en licensdata-meddelandesammanställning skapad genom att en hash utförs på licensdatan.

43. Ett system i enlighet med punkt **42**, vari den andra verifikationsdatabas består av en kopia av licensdata-meddelandesammanställningen.

44. Ett system i enlighet med punkt **43**, vari den elektroniska enheten är konfigurerad för att verifiera giltigheten hos licensmediet genom att jämföra licensdata-meddelandesammanställningen med kopian av licensdata-meddelandesammanställningen i den andra verifikations-databasen.

45. Ett system i enlighet med punkt **42**, vari licensdata-meddelandesammanställningen krypteras med en privat nyckel kopplad till registreringsinstansen eller licenshanteraren.

46. Ett system i enlighet med punkt **45**, vari den privata nyckeln är en av ett antal privata nycklar kopplade till registreringsinstansen eller licenshanteraren.

47. Ett system i enlighet med punkt **45**, vari den andra verifikationsdatabasen består av en kopia av den krypterade licensdata-meddelandesammanställningen.

48. Ett system i enlighet med punkt **47**, vari den elektroniska enheten är konfigurerad för att verifiera giltigheten hos licensmediet genom att jämföra den krypterade licensdata-meddelandesammanställningen med kopian av den krypterade licensdata-meddelandesammanställning i den andra verifikations-databasen.

49. Ett system i enlighet med punkt **47**, vari den elektroniska enheten är konfigurerad för att verifiera giltigheten hos licensmediet genom att:

avkryptera licensdata-meddelandesammanställningen som läses från licensmediet med hjälp av en allmän nyckel kopplad till registreringsinstansen;

generera en meddelandesammanställning genom att utföra en hash på licensdatan som läses från licensmediet; och

jämföra den avkrypterade meddelandesammanställningen med den genererade meddelandesammanställningen.

50. Ett system i enlighet med punkt **39**, vari licenshanteraren är konfigurerad för att skicka platslicens-registreringsinformation till registreringsinstansen.

51. Ett system i enlighet med punkt **50**, vari platslicensens registreringsinformation består av en slumpad identifierare kopplad till elektroniska data.

52. Ett system i enlighet med punkt **51**, vari den första verifikationsdatabasen består av en lista över behöriga identifierare som tillåter åtkomst till elektroniska data.

53. Ett system i enlighet med punkt **52**, vari registreringsinstansen är konfigurerad för att tillhandahålla uppdaterad verifikationsdata till licenshanteraren när identifieraren som skickas med registreringsinformationen överensstämmer med en av de behöriga identifierarna.

54. Ett system i enlighet med punkt **39**, vari licenshanteraren är konfigurerad för att kommunicera med registreringsinstansen för att verifiera att den andra verifikationsdatabasen överensstämmer med verifikationsdatabasen.

55. Ett system i enlighet med punkt **39**, vari licensdatan består av ett licensmedium-förfallodatum fastställt av en konfigurerbar tidsperiod under vilken licensmediet är giltigt.

56. Ett system i enlighet med punkt **39**, vari licensdatan består av ett mjukvarulicens-förfallodatum fastställt av en konfigurerbar tidsperiod under vilken åtkomst till elektroniska data är tillåten.

57. A system i enlighet med punkter **55** och **56**, vari licensmediets förfalloperiod är inställt till den kortaste förfalloperioden för mjukvarulicensen för licensdatan.

58. Ett system i enlighet med punkt **39**, vari licensdatan består av en mjukvarusäkerhets-förfallodatum fastställt av en konfigurerbar tidsperiod under vilken åtkomst till elektroniska data är tillåten.

59. Ett system i enlighet med punkt **39**, vari licensmediet är konfigurerat för att kommunicera med den elektroniska enheten genom en fast anslutning.

60. Ett system i enlighet med punkt **39**, vari licensmediet är konfigurerat för att kommunicera med den elektroniska enheten genom en trådlös anslutning

61. Ett system i enlighet med punkt **39**, vari licensmediet är konfigurerat för att kommunicera med den elektroniska enheten via ett nätverk.

62. Ett system i enlighet med punkt **61**, vari nätverket är Internet.

63. A system för att förhindra obehörig åtkomst till elektronisk data på en elektronisk enhet, systemet består av :

Lagringsmedel för licensdata konfigurerat för att kommunicera med den elektroniska enheten, licensdatan används för att fastställa om åtkomst till elektroniska data ska tillåtas;

Auktoriseringsmedel för registrering med ett första verifieringsmedel för verifiering av de licensdata som tillhandahålls av ett andra verifieringsmedel; och

licenshanteringsmedel konfigurerat för att kommunicera med den elektroniska enheten och registreringsauktoriseringsmedlet, licenshanteringsmedlet har det andra verifieringsmedlet för verifiering av licensdata lagrat på lagringsmedlet för licensdata,

vari är registreringsauktoriseringsmedlet konfigurerat för att tillhandahålla uppdaterade verifikationsdata för den andra verifikationsdatabasen hos licenshanteringsmedlet, och

licenshanteringsmedlet är konfigurerat för att tillhandahålla uppdaterad licensdata till lagringsmedlet för licensdata.

64. Ett system för att förhindra obehörig åtkomst till elektronisk data på en elektronisk enhet, systemet består av:

a Smartkort konfigurerat för att kommunicera med den elektroniska enheten och konfigurerat för att lagra licensdata, licensdatan används för att fastställa om åtkomst till elektroniska data ska tillåtas;

en registreringsserver har en första verifikationsdatabas för verifiering a licensdata lagrad i en andra verifikationsdatabas; och

a licenshanteringsserver konfigurerad för att kommunicera med den elektroniska enheten och registreringsservern , licenshanteringsservern har den andra verifikations-databasen för verifiering av licensdatan som lagras på Smartkortet,

vari registreringsservern är konfigurerad för att tillhandahålla uppdaterad verifikationsdata för den andra verifikationsdatabasen på licenshanterarservern, och

licenshanterarservern är konfigurerad för att tillhandahålla uppdaterad licensdata till smartkortet.

65. En registreringsinstans för att förhindra obehörig åtkomst till elektronisk data på en elektronisk enhet, registreringsinstansen består av:

medel för att kommunicera med licenshanteraren; och

En första verifikationsdatabas för verifiering av licensdata lagrad på en andra verifikationsdatabas på en licenshanterare som är konfigurerad för att kommunicera med den elektroniska enheten,

vari är den andra verifikationsdatabas konfigurerad för att verifiera licensdata lagrade på ett bärbart licensmedium som är konfigurerad för att kommunicera med den elektroniska enheten,

licensdatan är konfigurerad för att användas för att fastställa om åtkomst till elektroniska data ska tillåtas, och

registreringsinstansen är konfigurerad för att tillhandahålla uppdaterad verifikationsdata till den andra verifikationsdatabasen hos licenshanteraren.

66. Ett smartkort för att förhindra obehörig åtkomst till elektronisk data på en elektronisk enhet, smartkortet består av:

medel för att kommunicera med den elektroniska enheten;

ett minne för lagring av data mottagna från kommunikationsmedlet; och

licensdata lagrade i minnet, licensdatan konfigureras för att användas av den elektroniska enheten för att fastställa om åtkomst till elektroniska data ska tillåtas,

vari licensdatan har verifierats av en licenshanterings-verifikationsdatabas lagrad på en licenshanteringsserver konfigurerad för att kommunicera med den elektroniska enheten och en registreringsserver, och licenshanterings-verifikationsdatabasen har verifierats av en registreringsdatabas lagrad på registreringsservern, och

Smartkortet är konfigurerat för att ta emot uppdaterade licensdata från licenshanteringsservern.

67. En metod för att förhindra obehörig åtkomst till elektroniska data som lagras på en elektronisk enhet, metoden består av följande steg:

lagra licensdata på ett bärbart licensmedium konfigurerat för att kommunicera med den elektroniska enheten;

fastställa om åtkomst till elektroniska data ska tillåtas baserat på licensdatan;

verifiera licensdatan som lagras på licensmediet med hjälp av en registreringsinstans som har verifikationsdata och konfigureras för att kommunicera med den elektroniska enheten; och

tillhandahålla uppdaterade licensdata till licensmediet med hjälp av registreringsinstansen.

68. En metod i enlighet med punkt **67**, vari under verifieringssteget, den elektroniska enheten jämför licensdatan lagrad på licensmediet med verifikationsdatan.

69. En metod i enlighet med punkt **67**, vari licensmediet lagrar en licensdata-meddelandesammanställning skapad genom att en hash av licensdatan utförs.

70. En metod i enlighet med punkt **69**, vari verifikationsdatan består av en kopia av licensdata-meddelandesammanställningen.

71. En metod i enlighet med punkt **70**, vari under verifieringssteget, den elektroniska enheten jämför licensdata-meddelandesammanställningen som lagras på licensmediet med kopian av licensdata-meddelandesammanställningen i verifikationsdatan.

72. En metod i enlighet med punkt **69**, vari licensdata-meddelandesammanställningen krypteras med en privat nyckel kopplad till registreringsinstansen.

73. En metod i enlighet med punkt **72**, vari där den privata nyckeln är en av ett flertal privata nycklar kopplade till registreringsinstansen.

74. En metod i enlighet med punkt **72**, vari verifikationsdatan består av en kopia av den krypterade licensdata-meddelandesammanställningen.

75. En metod i enlighet med punkt **74**, vari i verifieringssteget, den elektroniska enheten jämför den krypterade licensdata-meddelandesammanställning lagrad på licensmediet med kopian av den krypterade licensdata-meddelandesammanställning in verifikationsdatan.

76. En metod i enlighet med punkt **72**, består dessutom av stegen:

att läsa licensdata-meddelandesammanställningen från licensmediet med hjälp av den elektroniska enheten;

avkryptera licensdata-meddelandesammanställningen med hjälp av en allmän nyckel kopplad till registreringsinstansen;

generera en meddelandesammanställning genom att utföra en hash på licensdatan som läses från licensmediet; och

jämföra den avkrypterade meddelandesammanställningen med den genererade meddelandesammanställningen.

77. En metod i enlighet med punkt **67**, består dessutom v steget med att skicka registreringsinformationen till registreringsinstansen med hjälp av den elektroniska enheten.

78. En metod i enlighet med punkt **77**, vari registreringsinformationen består av en slumpad identifierare som är kollad till elektroniska data.

79. En metod i enlighet med punkt **78**, vari verifikationsdatan består av en lista av behöriga identifierare som tillåter åtkomst till elektroniska data.

80. En metod i enlighet med punkt **79**, vari registreringsinstansen tillhandahåller uppdaterad licensdata till licensmediet när identifieraren som skickas med registreringsinformationen överensstämmer med en av de behöriga identifierarna.

81. En metod i enlighet med punkt **67**, vari licensmediet består av ett smartkort som har en mikroprocessor och ett minne.

82. En metod i enlighet med punkt **81**, vari smartkortet utför stegen med att:

Avkryptera en första meddelandesammanställning mottagen från registreringsinstansen med en allmän nyckel kopplad till registreringsinstansen;

Generera en andra meddelandesammanställning genom att utföra en hash på uppdaterad licensdata mottagen från registreringsinstansen; och

Jämföra den första meddelandesammanställningen med den andra meddelandesammanställningen.

83. En metod i enlighet med punkt **67**, vari licensdatan består av ett licensmedium-förfallodatum fastställt av en konfigurerbar tidsperiod under vilken licensmediet är giltigt.

84. En metod i enlighet med punkt **67**, vari licensdatan består av ett en mjukvarulicens-förfallodatum fastställt av en konfigurerbar tidsperiod under vilken åtkomst till elektroniska data är tillåten.

85. En metod i enlighet med punkter **83** eller **84**, vari licensmediets förfalloperiod är satt till den kortaste förfalloperioden för mjukvarulicensen för licensdatan.

86. En metod i enlighet med punkt **67**, vari licensdatan består av ett mjukvarusäkerhets-förfallodatum fastställt av en konfigurerbar tidsperiod under vilken åtkomst till elektroniska data är tillåten.

87. En metod för att förhindra obehörig åtkomst till elektroniska data lagrade på en elektronisk enhet, metoden består av följande steg:

lagra licensdata på ett bärbart licensmedium konfigurerat för att kommunicera med den elektroniska enheten;

fastställa om åtkomst till elektroniska data ska tillåtas baserat på licensdatan;

verifiera, med hjälp av en registreringsinstans som har en första verifikationsdatabas, licensdatan som lagras i en andra verifikationsdatabas;

verifiera licensdatan som lagras på licensmediet med hjälp av en licenshanterare som har den andra verifikationsdatabas och konfigureras för att kommunicera med den elektroniska enheten och registreringsinstansen;

tillhandahålla, med hjälp av registreringsinstansen, uppdaterad verifikationsdata för den andra verifikationsdatabasen på licenshanteraren; och

tillhandahålla licensdata till licensmediet med hjälp av licenshanteraren.

88. En metod i enlighet med punkt **87**, vari den elektroniska enheten verifierar licensmediets giltighet genom att jämföra licensdatan med den andra verifikationsdatabasen.

89. En metod i enlighet med punkt **87**, vari licenshanteraren verifierar giltigheten hos den andra verifikationsdatabas genom att jämföra den med den första verifikationsdatabas.

90. En metod i enlighet med punkt **87**, vari licensmediet lagrar en licensdata-meddelandesammanställning skapad genom att en hash utförs på licensdatan.

91. En metod i enlighet med punkt **90**, vari den andra verifikationsdatabasen består av en kopia av licensdata-meddelandesammanställningen.

92. En metod i enlighet med punkt **91**, vari den elektroniska enheten verifierar licensmediets giltighet genom att jämföra licensdata-meddelandesammanställningen med kopian av licensdata-meddelandesammanställningen i den andra verifikationsdatabasen.

93. En metod i enlighet med punkt **90**, vari licensdata-meddelandesammanställningen krypteras med en privat nyckel som är kopplad till registreringsinstansen eller licenshanteraren.

94. En metod i enlighet med punkt **93**, vari den privata nyckeln är en av ett flertal privata nycklar kopplade till registreringsinstansen eller licenshanteraren.

95. En metod i enlighet med punkt **93**, vari den andra verifikationsdatabasen består av en kopia av den krypterade licensdata-meddelandesammanställningen.

96. En metod i enlighet med punkt **95**, vari den elektroniska enheten bekräftar licensmediets giltighet genom att jämföra den krypterade licensdata-meddelandesammanställningen med kopian av den krypterade licensdata-meddelandesammanställning i den andra verifikationsdatabasen.

97. En metod i enlighet med punkt **95**, vari den elektroniska enheten verifierar licensmediets giltighet genom att:

avkryptera licensdata-meddelandesammanställningen som läses från licensmediet med hjälp av en allmän nyckel kopplad till registreringsinstansen;

generera en meddelandesammanställning genom att utföra en hash på licensdatan som läses från licensmediet; och

jämföra den avkrypterade meddelandesammanställningen med den genererade meddelandesammanställningen.

98. En metod i enlighet med punkt **87**, vari licenshanteraren skickar platslicens-registreringsinformation till registreringsinstansen.

99. En metod i enlighet med punkt **98**, vari platslicensens registreringsinformation består av en slumpad identifierare kopplad till elektroniska data.

100. En metod i enlighet med punkt **99**, vari den första verifikationsdatabas består av en lista över behöriga identifierare som tillåter åtkomst till elektroniska data.

101. En metod i enlighet med punkt **100**, vari registreringsinstansen tillhandahåller uppdaterad verifikationsdata till licenshanteraren när identifieraren som skickas tillsammans med registreringsinformationen överensstämmer med en av de behöriga identifierarna.

102. En metod i enlighet med punkt **87**, vari licenshanteraren kommunicerar med registreringsinstansen för att verifiera att den andra verifikationsdatabasen överensstämmer med den första verifikationsdatabasen.

103. En metod i enlighet med punkt **87**, vari licensdatan består av ett licensmedium-förfallodatum fastställt av en konfigurerbar tidsperiod under vilken licensmediet är giltigt.

104. En metod i enlighet med punkt **87**, vari licensdatan består av ett mjukvarulicens-förfallodatum fastställt av en konfigurerbar tidsperiod under vilken åtkomst till elektroniska data är tillåten.

105. En metod i enlighet med punkter **103** och **104**, vari licensmedie-förfalloperioden är ställd till den kortaste mjukvarulicens-förfalloperioden för licensdatan.

106. En metod i enlighet med punkt **87**, vari licensdatan består av ett en mjukvarusäkerhets-förfallodatum fastställt av en konfigurerbar tidsperiod under vilken åtkomst till elektroniska data är tillåten.

107. Datorkod utförbar på en elektronisk enhet för att förhindra obehörig åtkomst till elektroniska data lagrade på den elektroniska enheten, datorkoden består av:

Kod för lagring av licensdata på ett bärbart licensmedium konfigurerat för att kommunicera med den elektroniska enheten;

Kod för att fastställa om åtkomst till elektroniska data ska tillåtas baserat på licensdatan;

Kod för att verifiera licensdatan som är lagrad på licensmediet genom att kommunicera med en registreringsinstans som har verifikationsdatan; och kod för att tillhandahålla uppdaterade licensdata mottagna från registreringsinstansen till licensmediet.

108. Ett datorprogram utförbart på en elektronisk enhet för att tillhandahålla åtkomst till elektroniska data på den elektroniska enheten, datorprogrammet består av:

Kod för att förhindra åtkomst till elektroniska data; och

Ett underprogram för att förhindra obehörig åtkomst till elektroniska data, underprogrammet inkluderar:

Kod för att lagra licensdata på ett bärbart licensmedium konfigurerat för att kommunicera med den elektroniska enheten,

Kod för att fastställa om åtkomst ska tillåtas till elektroniska data baserat på licensdatan,

Kod för att verifiera licensdatan som lagras på licensmediet genom att kommunicera med en registreringsinstans som har verifikationsdata, och kod för att tillhandahålla uppdaterade licensdata mottagna från registreringsinstansen till licensmediet.

109. Datorkod utförbar på en elektronisk enhet för att förhindra obehörig åtkomst till elektroniska data lagrade på den elektroniska enheten, datorkoden består av:

Kod för att lagra licensdata på ett bärbart licensmedium konfigurerat för att kommunicera med den elektroniska enheten,

Kod för att fastställa om åtkomst ska tillåtas till elektroniska data baserat på licensdatan; kod för verifiering genom att kommunicera med en registreringsinstans som har en första verifikationsdatabas, licensdatan lagras i en andra verifikationsdatabas;

Kod för verifiering av licensdatan som lagras på licensmediet genom att kommunicera med en licenshanterare som har den andra verifikationsdatabasen och konfigureras för att kommunicera med den elektroniska enheten och registreringsinstansen;

Kod för att tillhandahålla uppdaterad verifikationsdata mottagen från registreringsinstansen till den andra verifikationsdatabas för licenshanteraren; och

Kod för att tillhandahålla licensdata mottagen från licenshanteraren till licensmediet.

110. Ett datorprogram utförbart på en elektronisk enhet för att tillhandahålla åtkomst till elektroniska data lagrade på den elektroniska enheten, datorprogrammet består av:

Kod för att ge åtkomst till elektroniska data; och

Ett underprogram för att förhindra obehörig åtkomst till elektroniska data, underprogrammet inkluderar:

Kod för att lagra licensdata på ett bärbart licensmedium konfigurerat för att kommunicera med den elektroniska enheten,

Kod för att fastställa om åtkomst ska tillåtas till elektroniska data baserat på licensdatan; ; kod för verifiering genom att kommunicera med en registreringsinstans som har en första verifikationsdatabas, licensdatan lagras i en andra verifikationsdatabas;

Kod för verifiering av licensdatan som lagras på licensmediet genom att kommunicera med en licenshanterare som har den andra verifikationsdatabasen och konfigureras för att kommunicera med den elektroniska enheten och registreringsinstansen;

Kod för att tillhandahålla uppdaterad verifikationsdata mottagen från registreringsinstansen till den andra verifikationsdatabas för licenshanteraren; och kod för att tillhandahålla licensdata mottagen från licenshanteraren till licensmediet.

111. En metod för användning av ett smartkort för att få tillgång till skyddade elektroniska data på en elektronisk enhet, metoden består av följande steg:

överföra licensdata som lagras på smartkortet till den elektroniska enheten; och

använda den elektroniska enheten för att fastställa, baserat på licensdatan, om åtkomst till elektroniska data ska tillåtas,

vari smartkortet är konfigurerat för att lagra uppdaterade licensdata hämtade från den elektroniska enheten eller från en fjärrenhet.

112. En metod för användning av ett smartkort för att få tillgång till skyddade elektroniska data på en elektronisk enhet, metoden består av följande steg:

Överföring av licensdata som lagras på smartkortet till den elektroniska enheten;

använda den elektroniska enheten för att fastställa, baserat på licensdatan, om åtkomst till elektroniska data ska tillåtas;

kommunicera, om åtkomst till elektroniska data inte tillåts, med en registreringsinstans som har verifikationsdata för att verifiera och/eller uppdatera de licensdata som är lagrade på smartkortet; och

på smartkortet lagra uppdaterade licensdata hämtade från registreringsinstansen.

113. En metod för användning av ett smartkort för att få tillgång till skyddade elektroniska data på en elektronisk enhet, metoden består av följande steg:

överföra licensdata som lagras på smartkortet till en registreringsinstans som har verifikationsdata för att verifiera licensdatan; och

från registreringsinstansen ta emot en fastställelse om åtkomst till elektroniska data ska tillåtas eller inte,

vari smartkortet är konfigurerat för att lagra uppdaterade licensdata mottagna från registreringsinstansen.

* * * * *